CHAPTER 6

NETWORKING HARDWARE

After reading this chapter and completing the exercises, you will be able to:

- Identify the functions of LAN connectivity hardware
- Install and configure a network adapter (network interface card)
- Identify problems associated with connectivity hardware
- Describe the factors involved in choosing a network adapter, hub, switch, or router
- Understand the functions of repeaters, hubs, bridges, switches, and gateways
- Describe the uses and types of routing protocols

ON THE JOB

As a network architect, I was asked to investigate why a large insurance company was experiencing performance degradation between campus buildings. This company was planning to expand its staff, but felt it needed to solve the network problem before adding any more users. The link between the buildings was fiber-optic cable, which should have provided plenty of capacity for mainframe data from one building to quickly reach the screens of claims processors at another building.

Realizing that wiring wasn't the problem, I looked at the connectivity hardware on the network. This network relied on a single router and 10 hubs for over 200 users. The router was software-based and ran on a Novell server (as opposed to a hardware-based router). Software-based routers are never as efficient as hardware-based routers; that was probably one bottleneck. In addition, having a network comprised of hubs and routers meant that all bandwidth was being shared by the devices. To cut down congestion, I replaced the router with a switch.

That replacement solved the performance problem. Now, instead of waiting three seconds for a screen to be refreshed, the insurance company employees get a new screen instantly after pressing the Enter key.

Carrie McClelland
ARK Consulting

In Chapter 4, you learned how data are transmitted over cable or through the atmosphere. Now you need to know how data arrive at their destination. To understand this process, it's helpful to compare data transmission to the means by which the U.S. Postal Service delivers mail: Mail trucks, airplanes, and delivery staff serve as the transmission media that move information from place to place. Machines and personnel at the post office interpret addresses on the envelopes and either deliver the mail to a transfer point or to your home. Inefficiencies in mail delivery, such as letters being misdirected to the wrong transfer point, frustrate both the sender and the receiver of the mail and increase the overall cost of delivery.

In data networks, the task of directing information to the correct destination in as efficient a manner as possible is handled by hubs, routers, bridges, and switches. In this chapter, you will learn about these devices and their roles in managing data traffic. Whereas earlier chapters focused mainly on the Physical layer of the OSI Model, this chapter delves into the Data Link and Network layers. It introduces the concepts involved in moving data from place to place, including issues related to switching and routing protocols. It also provides pictures of the hardware—repeaters, hubs, switches, bridges, and routers—that make data transfer possible. (It's important for you to have an accurate mental image of this equipment because, in a cluttered telecommunications closet, it may prove difficult to identify the hardware underneath the wiring.) In addition, you will learn all about network interface cards, which serve as the workstation's link to the network and are often the source of many connectivity problems.

Network Adapters

In Chapter 1, you learned that network adapters (also called network interface cards, or NICs) are connectivity devices that enable a workstation, server, printer, or other node to receive and transmit data over the network media. You also learned that in most modern network devices, network adapters contain the data transceiver, the device that transmits and receives data signals. NICs belong to both the Physical layer and Data Link layer of the OSI Model because they apply data signals to the wire and assemble or disassemble data frames. They do not, however, analyze the data from higher layers. For example, they could not determine whether the data they are transmitting and receiving are encoded nor could they decide how to decode them.

Advances in network adapter technology are making this hardware smarter than ever. Not only do all network adapters read addressing information so as to deliver data to their proper destination (and, in the case of Ethernet networks, to detect collisions), but many can also perform prioritization, network management, buffering, and traffic-filtering functions.

Network interface cards come in a variety of types depending on the logical topology (for example, Ethernet versus Token Ring), network transmission speed (for example, 10 Mbps versus 100 Mbps), connector interfaces (for example, BNC versus RJ-45), type of compatible system board or device, and, of course, manufacturer. Popular network adapter manufacturers include 3Com, Adaptec, D-Link, IBM, Intel, Kingston, Linksys, Netgear, SMC, and Western Digital, to name just a few. In fact, during your networking career, you may run into network adapters made by at least a dozen manufacturers.

As you learn about installing, configuring, and troubleshooting network adapters, you should concentrate first on generalities, then move on to special situations. Because network adapters are common to every networking device and every network, knowing all about them may prove to be the most useful tool you have at your disposal.

Types of Network Adapters

Before you order or install a network adapter in a network device, you need to know the type of interface required by the device. For a desktop or tower PC, the network adapter is likely to be a type of expansion board. An **expansion board** is a circuit board used to connect a device to the system board (the main circuit board that controls a computer, also known as a motherboard). Expansion boards connect to the system board through **expansion slots**, which are openings with multiple electrical contacts into which the expansion board can be inserted. Inserting an expansion board into an expansion slot establishes an electrical connection between the expansion board and the system board. Thus, the device connected to the expansion board becomes connected to the computer's main circuit. This connection enables the computer to centrally control its peripheral devices.

Expansion boards may also be called expansion cards, adapter cards, daughter cards, or daughter boards.

The circuit used by the system board to transmit data to the computer's components is the computer's **bus**. The type of expansion board, and therefore the type of network adapter you choose, must match the computer's bus. Buses differ according to their capacity. The capacity of a bus is defined principally by the width of its data path (expressed in bits) and its speed (expressed in MHz). A data path on a bus equals the number of data bits that it can transmit in parallel at any given time. In the earliest PCs, buses had an 8-bit data path. Later, manufacturers expanded buses to handle 16 bits of data, then 32 bits. Most new Pentium computers use buses capable of exchanging 64 bits of data, and some are even capable of 128 bits. As the number of bits of data that a bus can handle increases, so too does the speed of the devices attached to the bus.

In addition to the amount of data that can travel through their circuits, buses differ by type. The following list describes PC bus types you may encounter. (If you have already completed coursework for CompTIA's A+ certification, this material will look familiar.)

- *Industry Standard Architecture (ISA)*—The original PC bus, developed in the early 1980s to support an 8-bit and later 16-bit data transfer capability. 8-bit ISA (pronounced "ice-uh") bus connectors contain one long row of pins, and 16-bit ISA bus connectors add another, shorter row, for a second 8 bits, as shown in Figure 6-1. ISA buses cannot support 100-Mbps throughput; because of this limitation, they are typically not used for network adapters in new PCs, although they may still be found in "economy" PCs. ISA buses may connect serial devices, such as mice or modems, in new PCs.
- *MicroChannel Architecture (MCA)*—IBM's proprietary 32-bit bus for personal computers, introduced in 1987 and later replaced by the standardized EISA and PCI buses. Unless you are working in an IBM-centric environment with

older PS/2 or AIX equipment, you probably won't be concerned with MCA devices. Figure 6-1 shows an MCA network adapter.

- *Extended Industry Standard Architecture (EISA)*—A 32-bit bus that is compatible with older ISA devices because it shares the same length and pin configuration as the ISA bus, but that uses an extra layer of pins (resulting in a deeper, two-layered slot connector) for a second 16 bits to achieve faster throughput. An EISA expansion card is shown in Figure 6-1. The EISA (pronounced "ees-uh") bus was introduced in the late 1980s to compete with IBM's MCA bus.
- *Peripheral Component Interconnect (PCI)*—A 32- or 64-bit bus introduced in the 1990s that has become the network adapter connection type used for nearly all of today's new PCs. It's characterized by a shorter connector length than ISA, MCA, or EISA cards, but offers a much faster data transmission capability. PCI adapters are now standard for both PCs and Macintosh computers, allowing an organization to standardize on one make and model of NIC for use with all of their workstations. Figure 6-1 shows a typical PCI network adapter.

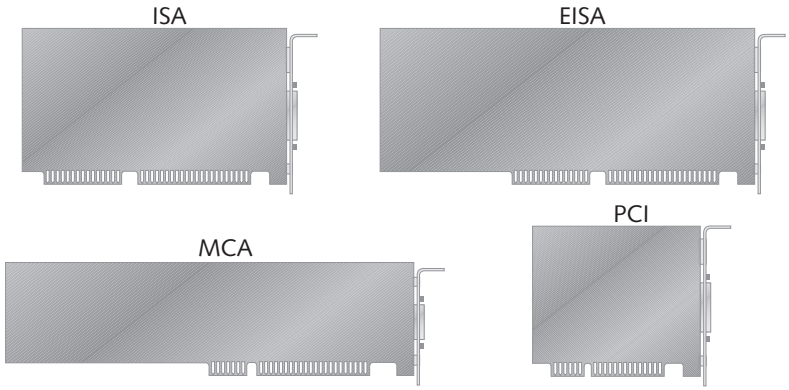


Figure 6-1 The four primary expansion card network adapters

You can easily determine what type of bus your PC uses by reading the documentation that came with the computer. This information should appear either on the purchase order or in the very beginning of the booklet that lists the computer's specifications. Someday, however, you may need to replace a network adapter on a PC whose documentation is missing. To verify what type of bus a PC uses, look inside the PC case. (Later in this chapter, you will learn how to safely open a computer case, check the computer's bus, and install a network adapter.) Most PCs have at least two different types of bus connections on the same board, as illustrated in Figure 6-2.

If a system board supports more than one kind of expansion slot, refer to the network adapter and PC manufacturers' guidelines for information on the preferred type of network adapter to install. If possible, you should choose a network adapter that matches the most modern bus on the system board. For example, if a PC supports both ISA and PCI, attempt to use a PCI network adapter. Although you may be able to use the older bus and network adapter types without any adverse effects, some network adapters (such as 3Com's products) will not work in an older bus if a faster, newer bus is available on the system board.

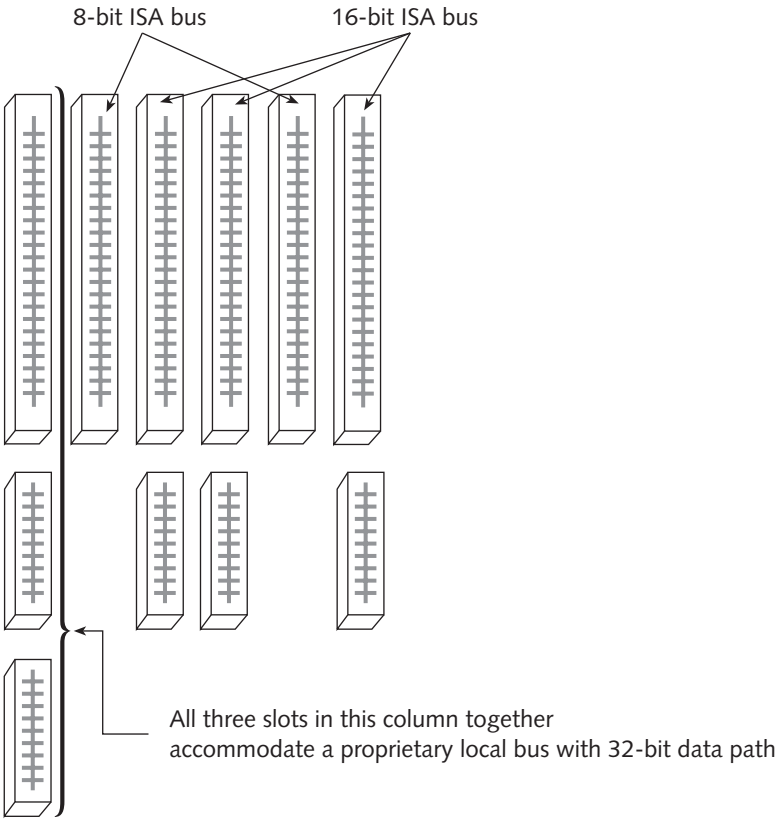


Figure 6-2 A system board with multiple bus types

Network adapters may connect to interfaces other than a PC's bus. For laptop computers, USB (universal serial bus) or Personal Computer Memory Card International Association (PCMCIA) slots may be used to connect network adapters; in older models of laptop computers, parallel ports may serve the same function. **PCMCIA** interfaces were developed in the early 1990s to provide a standard interface for connecting any type of device to a portable computer. PCMCIA devices are now more commonly known as **PC Cards**.

Some professionals also call them "credit card adapters" because they are approximately the same size as a credit card. PC Card slots may hold modem cards, network adapters, external hard disk cards, or CD-ROM cards. Most often, they are used for network adapters or modems; in fact, some PC Cards contain both devices. Figure 6-3 depicts a typical PC Card network adapter.

Figure 6-3 A typical PC Card network adapter

Another type of externally attached network adapter is one that relies on a **USB (universal serial bus) port**. USB is a standard external bus that can be used to connect multiple types of peripherals, including modems, mice, audio players, and network adapters. The original USB standard was developed in 1995 by a group of computer manufacturers working to make a low-cost, simple-to-install method of connecting peripheral devices to any make or model of computer. Since 1998, USB ports have been supplied on most modern laptop and desktop computers. The standard has become so popular that over 100 different types of devices have been designed to interface with the USB port.

One advantage to using a USB network adapter is its simple installation. A USB device needs only to be plugged into the USB port to be physically installed. An expansion board network adapter, on the other hand, requires the user to turn off the computer, remove its cover, insert the board into an expansion slot, fasten the board in place, replace the cover, and turn on the computer. Simple installation makes USB network adapters preferable for mobile users and novice users, such as those setting up a home network. However, the disadvantage of using a USB network adapter is that most USB ports in use today have a maximum data transfer rate of 12 Mbps (a newer high-speed USB standard that will support up to 480-Mbps throughput has been developed, but is not yet widely used). The traditional 12-Mbps limit means that a USB network adapter cannot be used on a network conforming to the 100BaseT standard unless the network's connectivity devices are capable of automatically adjusting between 10 Mbps and 100 Mbps. In any case, the USB port's throughput limitation makes this type of network adapter less desirable for networks on which data transfer speed is a critical variable. Figure 6-4 shows an example of a USB network adapter, which has a USB connector on one end and an RJ-45 receptacle on the other end.

Figure 6-4 A USB network adapter

A third type of externally attached network adapter is the parallel port network adapter. As the name implies, a parallel port network adapter attaches to the parallel port of a computer on one side and to the network cable (with a BNC or RJ-45 connector) on the other side. Parallel port network adapters were the first type of externally attached network adapter and were designed primarily for use on laptops. They enjoyed some popularity in the early 1990s. However, since the advent of PC Card and USB port network adapters, parallel port network adapters are rarely used on modern computers. In fact, these specialized devices can be difficult to obtain or support. The most popular parallel port network adapter manufacturer is Xircom. Figure 6-5 depicts a typical parallel port network adapter.

Figure 6-5 A parallel port network adapter

In addition to network adapters that connect with network cabling, you can employ network adapters designed for wireless transmission. Typically, a wireless network adapter uses

an antenna (either internal or external) to exchange signals with a base station transceiver or another wireless NIC. Expansion slot network adapters, PC Card network adapters and USB network adapters can all be wireless. However, the most popular type of wireless network adapter available today comes in the form of a PC Card network adapter.

Wireless network adapters are well suited to environments where cabling cannot be installed or in which clients need to move about while staying connected to the network. For example, library assistants can walk through stacks of books and record inventory data in the library's central database using handheld PCs require wireless connectivity. One disadvantage to using wireless network adapters is that they are generally more expensive than wire-dependent network adapters. Wireless connectivity manufacturers include 3Com, AMP, Cisco, ComStar, D-Link, Lucent, Proxim, Raytheon, and Webgear. Figure 6-6 depicts wireless PC Card and ISA network adapters.

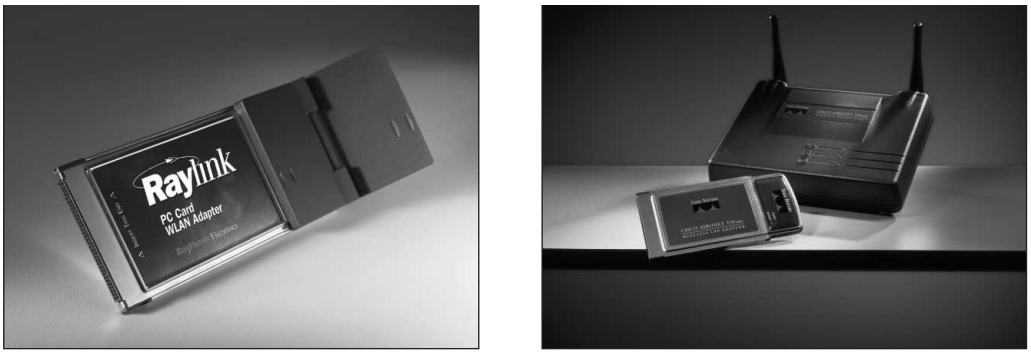


Figure 6-6 Wireless network adapters

As mentioned earlier, network adapters also vary by the type of logical topology they support (for example, Ethernet or Token Ring) and their connector types. Figure 6-7 shows a variety of network adapters that might be used on Ethernet networks, and Figure 6-8 shows a variety of network adapters designed for Token Ring networks. Notice that some network adapters provide only one type of cabling connector, while others provide two or even three types of connectors.

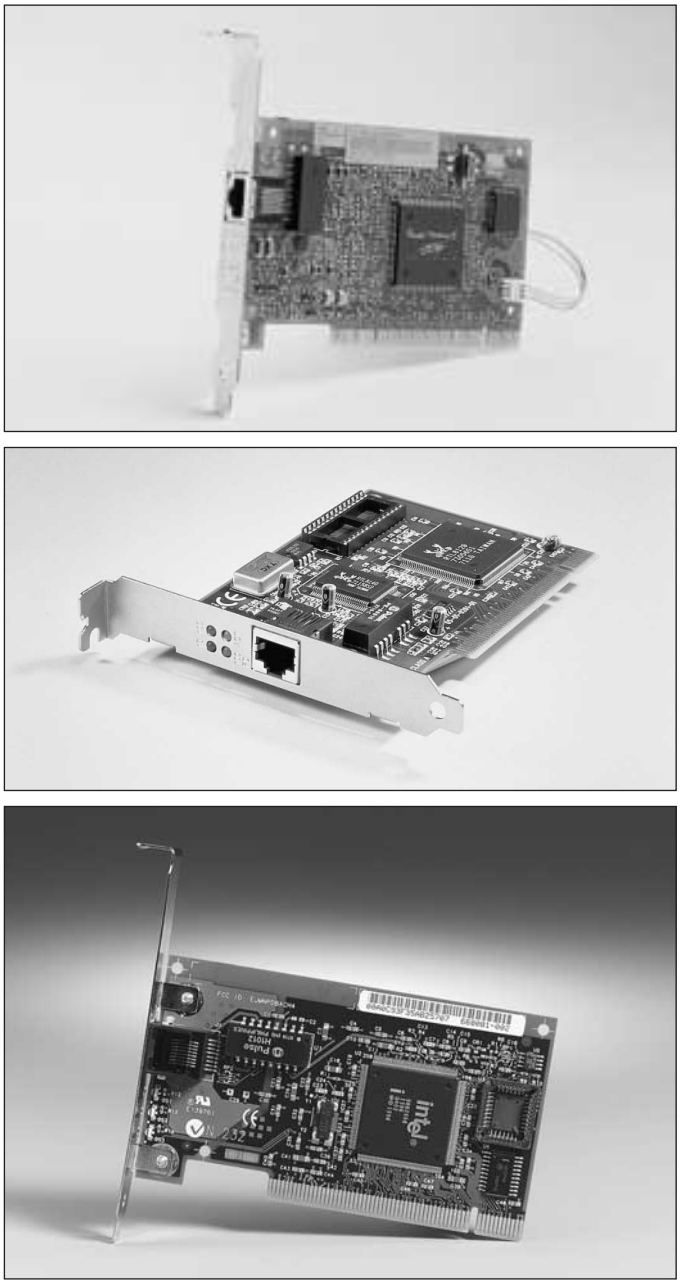
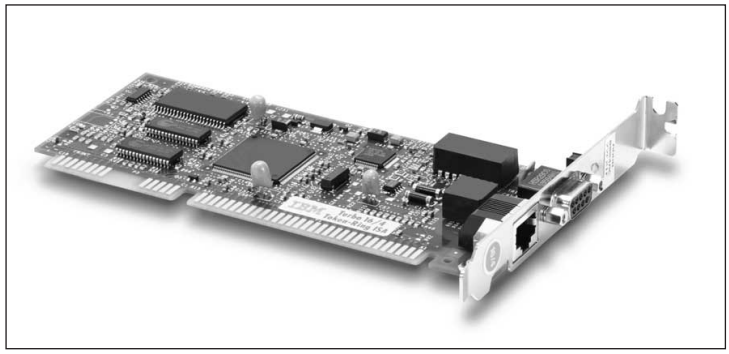


Figure 6-7 A variety of Ethernet network adapters



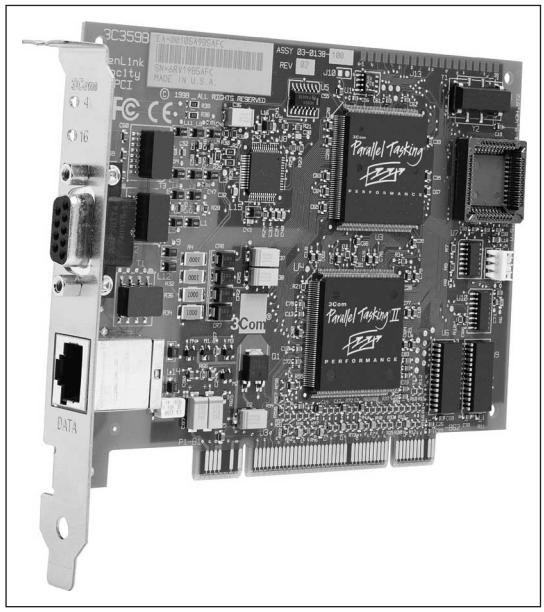


Figure 6-8 Token Ring network adapters

Devices other than PCs require specialized network adapters as well. Printer network adapters, for example, come in a variety of styles suited to different applications. By far, the most popular printer network adapter is Hewlett-Packard's JetDirect card. Printer network adapters often provide processing and support for all seven OSI Model layers (making them even more complex than PC network adapters) so as to handle print server functions. Figure 6-9 depicts typical Ethernet network adapters for networked printers.

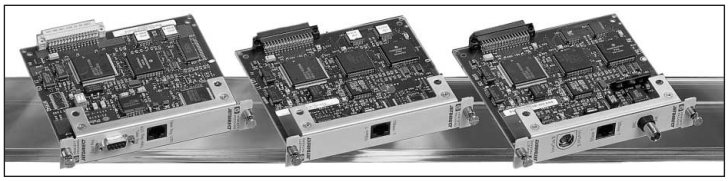


Figure 6-9 Ethernet network adapters for printers

Installing Network Adapters

To install a modern network adapter, you must first install the hardware, and then install the software that shipped with the NIC. In some cases, you may also have to perform a third step: configuring the **firmware**, which is a combination of hardware and software. The hardware component of firmware is a read-only memory (ROM) chip (built into the NIC) that stores data established at the factory. The ROM may be changed by configuration utilities (the software component of firmware) that come with the network adapter. Because its data can be erased or changed by applying electrical charges to the chip (via the software program), this particular type of ROM is called **electrically erasable programmable read-only memory (EEPROM)**.

A network adapter's firmware contains information about its transmission speed capabilities, its preferred IRQ (discussed later in this chapter) and input/output (I/O) port address, and duplexing capabilities, among other things. In many cases, especially if you are using Windows 2000 plug-and-play technology, you will not have to change the network adapter's firmware.

The following sections explain the steps involved in installing an expansion board network adapter, as well as how to install externally attached network adapters.

Installing and Configuring Network Adapter Hardware

As with any hardware installation, you should first read the manufacturer's documentation that accompanies the network adapter hardware. The following steps generally apply to any kind of expansion card network adapter installation (in a desktop computer), but your experience may vary.

To install an expansion card network adapter:

1. Make sure that your toolkit includes a Phillips-head screwdriver, a ground strap, and a ground mat to protect the internal components from electrostatic discharge. Also, make sure that you have ample space in which to work, whether it be on the floor, a desk, or table.
2. Turn off the computer's power switch, and then unplug the computer. In addition to endangering you, opening a PC while it's turned on can damage its internal circuitry.

3. Attach the ground strap to your wrist and make sure that it's connected to the ground mat underneath the computer.
4. Open the computer's case. Desktop computer cases are attached in several different ways. They might use four or six Phillips-head screws to attach the housing to the back panel or they might not use any screws and slide off instead. Remove all necessary screws and slide the computer's case off.
5. Select a slot on the computer's system board where you will insert the network adapter. Make sure that the slot matches the type of expansion card you have. Remove the metal slot cover for that slot from the back of the PC. Some slot covers are attached with Phillips-head screws; others are merely metal parts with perforated edges that you can punch out with your fingers.
6. Insert the network adapter by lining up its slot connector with the slot and pressing it firmly into the slot. Don't be afraid to press down hard, but make sure the expansion card is properly aligned with the slot when you do so. If you have correctly inserted the network adapter, you should not be able to wiggle it from side to side. If you can wiggle it, press it in farther. A loose network adapter will cause connectivity problems. Figure 6-10 depicts a properly inserted network adapter.

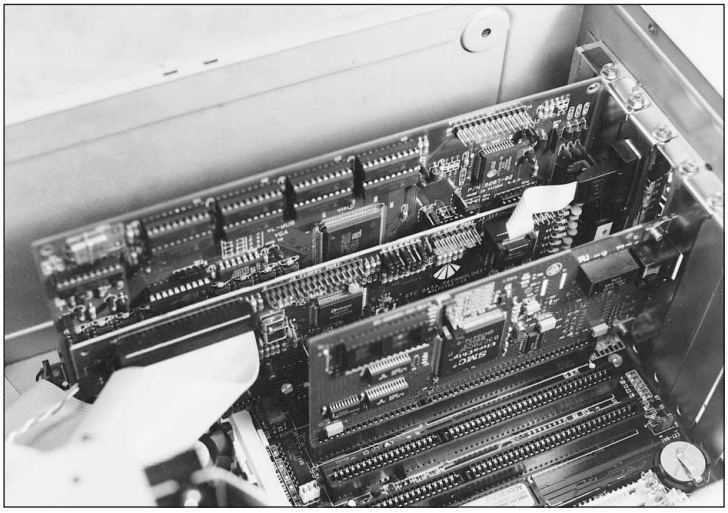


Figure 6-10 A properly inserted network adapter

7. The metal bracket at the end of the network adapter should now be positioned where the metal slot cover was located before you removed the slot cover. Attach the bracket with a Phillips-head screw to the back of the computer cover to secure the network adapter in place.

8. Make sure that you have not loosened any cables or cards inside the PC or left any screws or debris inside the computer.
9. Replace the cover on the computer and reinsert the screws that you removed in Step 4, if applicable.
10. Plug in the computer and turn it on. Proceed to configure the network adapter's software, as discussed later in this chapter.

Installing a PC Card network adapter is much easier than installing an expansion card network adapter. In general, you can simply turn off the machine, insert the PC Card into the PC Card slot, as shown in Figure 6-11, then turn on the computer. Most modern operating systems (such as Windows 2000) allow you to insert and remove the PC Card adapter without restarting the machine. Make sure that the PC Card is firmly inserted. If you can wiggle it, you need to push it in farther.

Figure 6-11 Installing a PC Card network adapter

Physically installing other types of external network adapters, such as parallel port or USB port adapters, is similar. All you need to do is insert the device into the computer's port, making sure that it is securely attached.

On servers and other high-powered computers, you may need to install multiple network adapters. For the hardware installation, you can simply repeat the installation process for the first network adapter, choosing a different slot. The trick to using multiple network adapters on one machine lies in correctly configuring the software for each network adapter. Simple network adapter configuration is covered in the following section. The exact steps involved in configuring network adapters on servers will depend on the server's networking operating system. Chapters 8 and 9 will describe the network

adapter configuration process for servers running the Windows 2000 Server and NetWare network operating systems.

On older expansion board network adapters, rather than using firmware utilities to modify settings, you may need to use, or set, a jumper. A **jumper** is a small, removable piece of plastic that contains a metal receptacle. This metal receptacle fits over a pair of pins on a circuit board to form a bridge that completes a circuit between those two pins. By moving the jumper from one set of pins to another set of pins, you can modify the board's circuit, thereby giving it different instructions. Jumper settings may be used to indicate an "on/off" situation or in more complex configurations, they may indicate one of multiple options. Figure 6-12 depicts how a jumper and a row of three pins can be used to indicate two different settings.

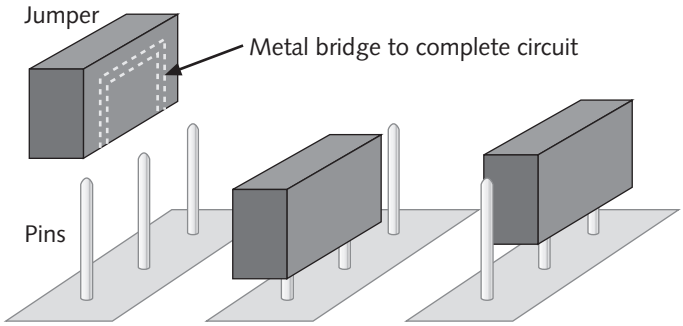


Figure 6-12 A jumper and a row of pins indicating two different settings

Jumpers are still used on hard drive controllers and system boards today, but rarely on modern network adapters. However, older NICs (such as those manufactured up to the mid-1990s) may use jumpers to modify their settings, including their transmission rate and duplexing capabilities. If you work on a network adapter that uses jumpers in its configuration, you must have the adapter's documentation in order to know which jumper settings correspond to which parameter setting. Jumper settings on one type of NIC will likely be different from those on another type of NIC.

Another method of changing parameters on a network adapter is by modifying the position of a DIP (dual inline package) switch. A **DIP switch** is a small, plastic toggle switch that can represent an "on" or "off" status. This status indicates a parameter setting. Just as with jumpers, DIP switches may be used to modify system resource settings such as the NIC's IRQ or other settings such as its maximum transmission speed. And as with jumpers, DIP switches are rarely used on modern NICs. You must have the documentation for the adapter in order to know which DIP switch settings represent a particular configuration. Figure 6-13 depicts a row of DIP switches on a NIC.

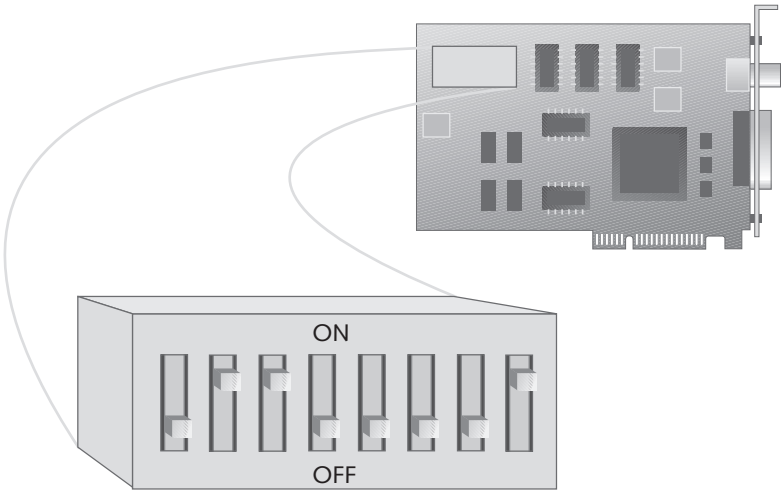


Figure 6-13 DIP switches on a NIC

Jumpers and DIP switches are both small and somewhat fragile components of a circuit board and as such, require care when handling. Jumpers can be easily dropped and are so small that they may get lost. One way to avoid this is to handle them with tweezers. DIP switches can be broken if they are handled roughly. To change the position of a DIP switch, you can use the tip of a paperclip or a small screwdriver.

Installing and Configuring Network Adapter Software

Even if your computer runs Windows 2000, Windows 9x, or an older Windows operating system with plug-and-play technology, you must ensure that the correct device driver is installed for the network adapter and that it is configured properly. A **device driver** is software that enables an attached device to communicate with the computer's operating system. When you purchase a computer that already contains an attached peripheral (such as a sound card), the device drivers should already be installed. However, when you add hardware, you must install the device drivers too. Some operating systems, such as Windows 2000, come with a multitude of built-in device drivers. In that case, after you physically install new hardware and reboot, the operating system will automatically recognize the hardware and install the device's drivers. Each time a computer boots up, the device drivers for all its connected peripherals are loaded into RAM so that the computer can communicate with those devices at any time.

In other cases, the operating system might not contain appropriate device drivers for the hardware you've added. This section describes how to install and configure network adapter software on a Windows 2000 Professional desktop operating system that does not contain the correct device drivers. For other operating systems, the process will be similar. Regardless of which operating system you use, you should first refer to the network

adapter's documentation, because your situation may vary. Read the network adapter documentation carefully before installing the relevant drivers, and make sure you are installing the appropriate drivers. Performing a Windows 95 installation on a Windows 2000 computer, for example, may cause problems.

The following steps describe a typical network adapter software installation from a Windows 2000 interface. For this process, you will need access to the Windows 2000 software (via either a Windows 2000 CD or hard disk) and the floppy disk that came with the network adapter. This floppy disk should contain device drivers specific to your network adapter.

If you do not have the floppy disk that shipped with the network adapter and the Windows 2000 software does not supply device drivers for your network adapter, you can download the network adapter software from the manufacturer's Web site. If you choose this option, make sure that you get the appropriate drivers for your operating system and network adapter type. Also, make sure that the drivers you download are the most current version (sometimes called "shipping drivers") and not beta-level (unsupported) drivers.

To install and configure NIC software:

1. Physically install the network adapter, and then restart the PC.
2. As long as you haven't disabled the plug-and-play technology in the computer's CMOS settings, Windows 2000 should automatically detect the new hardware. Upon detecting the network adapter, it should also install the NIC's driver. In many cases, you need not install any other software or adjust the configuration in order for the NIC to operate properly.
3. There are certain situations in which you might want to change or update the device driver that the operating system has chosen, however. To do this, right-click the **My Computer** icon and click **Properties**. The System Properties dialog box appears. (You may also reach the System Properties dialog box as follows: click Start, point to Settings, click Control Panel, and then double-click the System icon.)
4. Click the **Hardware** tab.
5. Click the **Device Manager** button.
6. The Device Manager window opens, with a list of installed devices. Double-click the **Network adapters** icon. A list of installed network adapters appears.
7. Double-click the adapter for which you want to install new device drivers. The network adapter's Properties dialog box appears.
8. Select the **Driver** tab. Details about your network adapter's current driver appear.

9. Click **Update Driver**. A Windows 2000 wizard appears to walk you through the device driver update process.
10. Click **Next** to continue. You are asked to choose whether you want Windows to select the most appropriate driver or whether you want to be prompted for suitable drivers.
11. Click the "Display a list of the known drivers for this device so that I can choose a specific driver" radio button, then click **Next** to continue. You are asked to choose the network adapter for which you want to install a new driver, as shown in Figure 6-14.

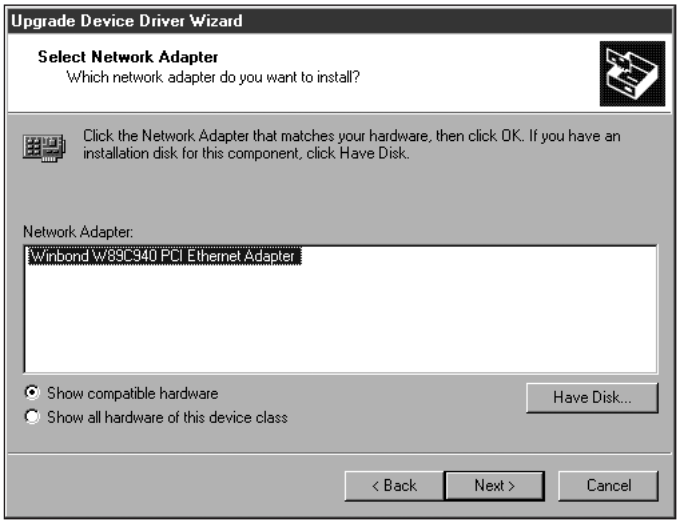


Figure 6-14 Windows 2000 Upgrade Device Driver Wizard

12. If your computer has more than one NIC, click the one whose drivers you want to upgrade, then click **Have Disk**. The Install from Disk dialog box appears.
13. Insert the disk that came with the network adapter into your floppy drive.
14. You will be prompted to enter the path for the appropriate driver or click **Browse** to find the driver's directory on your disk. The drivers will probably appear in a subdirectory on the disk, because most network adapters ship with a single disk that contains drivers for multiple platforms. Once you select the correct path, click **OK**.
15. If the disk sent with the network adapter contains drivers for more than one type of network adapter, you will be asked to select the precise model you are using. After making your choice, click **OK**.

16. The driver files for the network adapter will be installed onto your hard disk and their specifications written to the Registry. In the process, you may be asked for the location of the Windows 2000 system files. If so, insert the Windows 2000 installation CD. When prompted, direct the installation program to that drive (usually D:, E:, or F:), then click **OK**.
17. Once the network adapter drivers have been successfully installed, you will be prompted to restart your PC. Confirm that you want to restart it by clicking **Yes**.

The preceding steps will work in most situations. Because every situation is different, however, you should always read the manufacturer's documentation and follow its installation instructions. Some manufacturers supply setup programs that automatically install and register network adapter software once you run them, thereby eliminating the need to follow the steps outlined above.

The next sections describe the variable settings you should understand when configuring network adapters. Depending on your computer's use of resources, network adapter configuration may or may not be necessary after installation. For troubleshooting purposes, however, you need to understand how to view and adjust these variables. If you completed coursework for the A+ certification or have worked with PCs in the past, you should already be familiar with these variables.

IRQ (Interrupt Request) When a device attached to a computer's bus, such as a keyboard or floppy disk drive, requires attention from the computer's processor, it uses an interrupt request. An **interrupt request (IRQ)**, as its name implies, is a message to the computer that instructs it to stop what it is doing and pay attention to something else. An **interrupt** is the wire on which a device issues voltage to signal this request. Each interrupt must have a unique **IRQ number**, a number that uniquely identifies that component to the main bus. An IRQ number is the means by which the bus understands which device to acknowledge. The term "IRQ" is frequently substituted for "IRQ number" in casual conversation, even though they are technically two different things.

IRQ numbers range from 0 to 15. Many computer devices reserve the same IRQ number by default no matter what type of system. For example, on every type of computer, a floppy disk controller claims IRQ 6 and a keyboard controller takes IRQ 1. On the other hand, some IRQ numbers are not reserved by default, but are available to additional devices such as sound cards, graphics cards, modems, and network adapters. Most often, network adapters will use IRQ 9, 10, or 11. In order to obtain Network+ certification, you should be familiar with the IRQ numbers reserved by common computer devices as well as those most apt to be used by network adapters. Table 6-1 lists all of the IRQ numbers and their default device assignments, if they have any.

Table 6-1 IRQ assignments

IRQ Number	Typical Device Assignment
0	System timer (only)
1	Keyboard controller (only)
2	Access to IRQs 8–15
3	COM2 (second serial port) or COM4 (fourth serial port)
4	COM1 (first serial port) or COM3 (third serial port)
5	Sound card or LPT2 (second parallel port)
6	Floppy disk drive controller
7	LPT1 (parallel port 1)
8	Real-time clock (only)
9	No default assignment
10	No default assignment
11	No default assignment
12	PS/2 mouse
13	Math coprocessor (only)
14	IDE channel (for example, an IDE hard disk drive)
15	Secondary IDE channel

Generally, if two devices attempt to use the same interrupt, resource conflicts and performance problems will result. For example, if a keyboard uses IRQ number 1 and you configure the network adapter to use IRQ number 1 as well (if the operating system allows you do this), the computer's CPU will not know whether the request received through interrupt number 1 comes from the computer or the network adapter; thus the CPU will be unable to follow the instructions of either device.

Some plug-and-play devices are designed to coexist with other devices on the same IRQ. In such a situation, having two or more devices assigned to the same IRQ may not present a problem.

If IRQ conflicts occur, you must manually reassign a device's IRQ. Keep in mind that the BIOS or the operating system will attempt to assign free IRQs. Typically, it will assign IRQs 9, 10, or 11 to network adapters, because other devices do usually not take these numbers. The BIOS or the operating system can be wrong, however.

When two devices attempt to use the same IRQ, any of the following problems may occur:

- The computer may lock up or "hang" either upon starting or when the operating system is loading.
- The computer may run much more slowly than usual.

- Although the computer's network adapter may work properly, other devices—such as serial or parallel ports—may stop working.
- Video or sound card problems may occur. For example, after the operating system loads, you may see an error message indicating that the video settings are incorrect, or your sound card may stop working.
- The computer may fail to connect to the network (as evidenced by an error message after you attempt to log onto a server).
- The computer may experience intermittent data errors during transmission.

To view IRQ settings on computers running Windows 2000 Professional:

1. Right-click the **My Computer** icon. A shortcut menu opens.
2. Click **Properties**. The System Properties dialog box opens.
3. Click the **Hardware** tab.
4. Click the **Device Manager** button. The Device Manager window appears.
5. In the Device Manager menu bar, click **View**, and then click **Resources by connection**. A list of the system resources appears
6. Double-click the **Interrupt request (IRQ)** option to view your computer's IRQ assignments, as shown in Figure 6-15.

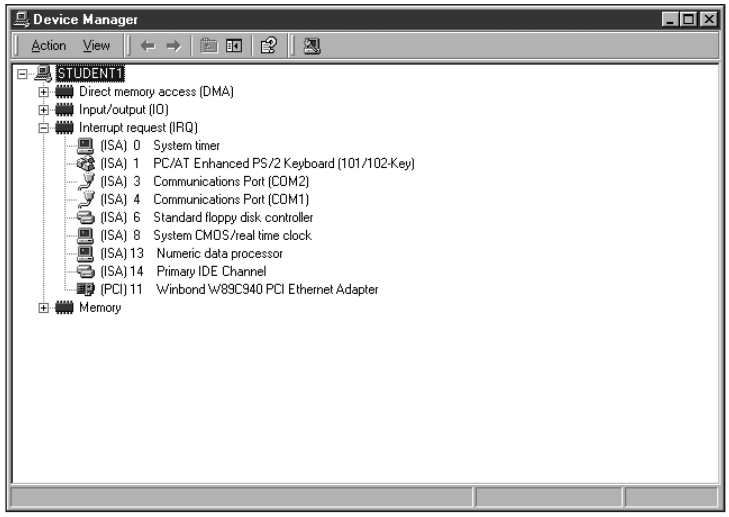


Figure 6-15 Computer resource settings in Windows 2000

You can also view IRQ settings in the computer's CMOS utility. **CMOS (complementary metal oxide semiconductor)** is a type of microchip that requires very little energy to operate. In a PC, the CMOS holds settings pertaining to the configuration

of a computer's devices, among other things. These settings are saved even after you turn off a PC because the CMOS is powered by a small battery in your computer. Information saved in CMOS is used by the computer's **BIOS (basic input/output system)**. The BIOS is a simple set of instructions that enables a computer to initially recognize its hardware. When you turn on a computer, the BIOS performs its start-up tasks. Once a computer is up and running, the BIOS provides an interface between the computer's software and hardware, allowing it to recognize which device is associated with each IRQ.

Although you can usually modify IRQ settings in the CMOS utility, whether you can change them from the operating system software depends on the type of network adapter involved. For example, on a PCI network adapter, which requires a PCI bus controller, the PCI controller's settings will dictate whether this type of modification is possible. The default setting prevents you from changing the network adapter's IRQ from the operating system; if you attempt to make this change on a Windows 2000 computer, for example, in the Resources tab in the PCI network adapter's Properties dialog, a box titled "No modifications allowed" will display the following message: "This resource setting cannot be modified."

Thus, if you need to alter the IRQ for a PCI network adapter, you should make the change in the CMOS. Different system board manufacturers use different keystrokes to invoke the CMOS setup program when the computer starts. You may need to press Del, Shift-F1, F10, Ctrl-Shift-Enter, or another key (or set of keys) to access the CMOS setup utility. The required keystroke or combination of keystrokes should appear on the screen shortly after the computer starts. Once you are in the CMOS setup utility, follow the menu selections until you find the network adapter IRQ setting, change it, then save your changes and restart the computer.

Sometimes you cannot access a computer's CMOS setup utility. In this case, you *may* be able to resolve an IRQ conflict by physically moving the network adapter from its present slot to another slot, by physically resetting dip switches on the network adapter, or by using a special setup program that is shipped with the network adapter. You could also try temporarily disabling or removing conflicting devices such as infrared ports or modems. Alternately, you may need to update the BIOS on the workstation. If nothing else works, you may need to install a different type or model of network adapter.

Memory Range The **memory range** indicates, in hexadecimal notation, the area of memory that the network adapter and CPU will use for exchanging, or buffering, data. As with IRQs, some memory ranges are reserved for specific devices—most notably, the system board. Reserved address ranges should never be selected for new devices.

Network adapters typically use a memory range in the high memory area, which in hexadecimal notation equates to the A0000–FFFFF range. As you work with network

adapters, you will notice that some manufacturers prefer certain ranges. For example, a 3Com PC Card adapter might, by default, choose a range of C8000–C9FFF. An IBM Token Ring adapter might choose a range of D8000–D9FFF.

Memory range settings are less likely to cause resource conflicts than IRQ settings, mainly because there are more available memory ranges than IRQs. Nevertheless, you may run into situations in which you need to change a network adapter's memory address. In such an instance, you may or may not be able to change the memory range from the operating system. Refer to the manufacturer's guidelines for instructions.

Base I/O Port The **base I/O port** setting specifies, in hexadecimal notation, which area of memory will act as a channel for moving data between the network adapter and the CPU. Like its IRQ, a device's base I/O port cannot be used by any other device. Most network adapters use two memory ranges for this channel, and the base I/O port settings identify the beginning of each range. Although a network adapter's base I/O port will vary depending on the manufacturer, some popular addresses (in hexadecimal notation) are 300 (which means that the range is 300–30F), 310, 280, or 2F8.

You will probably not need to change a network adapter's base I/O port. If you do, bear in mind that, as with IRQ settings, base I/O port settings for PCI cards can be changed in the computer's CMOS setup utility or sometimes through the operating system.

Firmware Settings Once you have adjusted the network adapter's system resources, you may need to modify its transmission characteristics—for example, whether it uses full duplexing or whether it can detect a network's speed. These settings are held in the adapter's firmware. As mentioned earlier, firmware comprises the combination of an EEPROM chip on the network adapter and the data it holds. When you change the firmware, you are actually writing to the EEPROM chip on the network adapter. You are not writing to the computer's hard disk. Although most configurable settings can be changed in the operating system or network adapter setup software, you may encounter complex networking problems that require a change to firmware settings.

To change a network adapter's firmware, you will need a bootable floppy disk (DOS version 6.0 or higher) containing the configuration or DOS install utility that shipped with the network adapter. If you don't have the utility, you can usually download it from the manufacturer's Web site. To run the utility, you must start the computer with this floppy disk inserted. The network adapter configuration utility may not run if an operating system or memory management program is already running.

Each configuration utility will differ slightly, but all should allow you to view the IRQ, I/O port, base memory, and node address. Some may allow you to change settings such as the network adapter's CPU utilization, its ability to handle full duplexing, or its capability to be used with only 10BaseT or 100BaseT media, for example (although many of these

can also be changed through the network adapter's properties from the operating system interface). The changeable settings will vary depending on the manufacturer. Again, read the manufacturer's documentation to find out the details for your hardware.

Network adapter configuration utilities also allow you to perform diagnostics—tests of the network adapter's physical components and connectivity. Most of the tests can be performed without additional hardware. However, in order to perform the entire group of the diagnostic tests on the NIC's utility disk, you must have a loopback plug. A **loopback plug** is a connector that plugs into a port, such as a serial or parallel or an RJ-45 port, and crosses over the transmit line to the receive line so that outgoing signals can be redirected back into the computer for testing. One connectivity test, called a loopback test, requires you to install a loopback plug into the network adapter's media connector. Note that none of the connectivity tests should be performed on a live network. If a network adapter fails its connectivity tests, it is probably configured incorrectly. If a network adapter fails a physical component test, it may need to be replaced.

The word loopback implies that signals are routed back toward their source, rather than toward an external destination. When used in the context of network adapters, the loopback test refers to a check of the adapter's ability to transmit and receive signals. Recall that the term "loopback" is also used in the context of TCP/IP protocol testing. In that context, pinging the loopback address provides you with information on TCP/IP functionality.

Choosing the Right Network Adapter

You should consider several factors when choosing a network adapter for your workstation or server. Of course, the most critical factor is compatibility with your existing system. You will need to determine whether your workstation requires an ISA, EISA, MCA or PCI card in addition to choosing a network adapter that matches your network's media, connector types, transmission speed, and network model. You also need to ensure that drivers available for that network adapter will work with your operating system.

Beyond these considerations, however, you should examine more subtle differences, such as those that affect network performance. Table 6-2 lists some features available on network adapters that specifically influence performance and ease of use. As you review this table, keep in mind that performance is especially important if the network adapter will be installed in a server.

Table 6-2 Network adapter characteristics

NIC Feature	Function	Benefit
Automatic speed selection	Enables NICs to automatically sense and adapt to a network's speed and mode (half- or full-duplex)	Aids configuration and performance
One or more on-board NIC CPU	Allows the card to perform some data processing independently of the PC's CPU	Improves performance
Direct Memory Access (DMA)	Enables the card to directly transfer data to the computer's memory	Improves performance
Diagnostic LEDs (lights on the NIC)	Indicate traffic, connectivity, and, sometimes, speed	Aid in troubleshooting (for more information, see Chapter 12)
Dual channels	Effectively creates two NICs in one slot	Improves performance; suited to servers
Load balancing	Allows the NIC's processor to determine when to switch traffic between internal cards	Improves performance for heavily-trafficked networks; suited to servers
"Look Ahead" transmit and receive	Allows the NIC's processor to begin processing data before it has received the entire packet	Improves performance
Management capabilities (SNMP)	Allows the NIC to perform its own monitoring and troubleshooting, usually through installed application software	Aids in troubleshooting, can find a problem before it becomes dire
Power management capabilities	Allows a NIC to participate in the computer's power saving measures; found on PC Card	Increases the life of the battery for laptop computers
RAM buffering	Provides additional memory on the NIC, which in turn provides more space for data buffering	Improves performance
Upgradeable (flash) ROM	Allows on-board chip memory to be upgraded	May improve ease of use and performance

The quality of the printed documentation that you receive from a manufacturer about its network adapters may vary. What's more, this documentation may not apply to the kinds of computers or networking environments you are using. To find out more about the type of network adapter you are installing or troubleshooting, visit the manufacturer's Web site.

REPEATERS

Now that you have learned about the many types of network adapters and how to install and configure them, you are ready to learn about connectivity devices. As you'll recall from Chapter 4, the telecommunications closet is the area containing the connectivity equipment (usually for a whole floor of a building). Within the telecommunications closet, horizontal cabling from the workstations attaches to punch-down blocks, patch panels, hubs, switches, routers, and bridges. In addition, telecommunications closets may house repeaters. As you learned in Chapter 4, repeaters are the connectivity devices that regenerate a digital signal.

Repeaters operate in the Physical layer of the OSI Model and, therefore, have no means to interpret the data they retransmit. For example, they cannot improve or correct a bad or erroneous signal; they merely repeat it. In this sense, they are not "intelligent" devices. Since they cannot read higher-layer information in the data packets, repeaters cannot direct data to their destination. Instead, repeaters simply regenerate a signal over an entire segment. It is up to the receiver to recognize and accept its data.

A repeater is limited not only in function, but also in scope. A repeater contains one input port and one output port, as shown in Figure 6-16, so it is capable of receiving and repeating only the data stream. Furthermore, repeaters are suited only to bus topology networks. The advantage to using a repeater is that it allows you to extend a network inexpensively.

For example, suppose that you need to connect a single PC located in a school's gymnasium to the rest of the network, that the nearest data jack is 220 meters away, and that you are using 10Base2 Ethernet, which limits the maximum cable length to 185 meters. In this instance, you could use a repeater to add 185 meters to the existing 185-meter limitation and connect the gymnasium workstation to the network. Bear in mind that the overall network distance limitations still apply. Because the entire network cannot exceed 1000 meters, you cannot use more than five repeaters in sequence to extend the cabling's reach.

Figure 6-16 Repeaters

HUBS

At its most primitive, a **hub** is a multiport repeater. A simple hub may contain multiple ports that can connect a group of computers in a peer-to-peer fashion, accepting and repeating signals from each node. A slightly more sophisticated hub may contain multiple ports for devices and one port that connects to a network's backbone. On Ethernet networks, hubs typically serve as the central connection point for branches of a star or star-based hybrid topology. On Token Ring networks, hubs are called Multistation Access Units (MAUs) and are used to connect nodes in a star-based ring topology. As you learned in Chapter 5, MAUs internally complete the ring topology using their Ring In and Ring Out ports.

In addition to connecting Macintosh and PC workstations, hubs can connect print servers, switches, file servers, or other devices to a network. They can support a variety of different media and data transmission speeds. Some hubs also allow for multiple media connector types or multiple data transmission speeds. As you can imagine, you can choose from a huge number of different hubs. By classifying hubs into categories according to their uses and features, however, you will quickly get the lay of the land and soon learn to understand any hub. Figure 6-17 details the various elements of a hub, some of which are optional. The elements shared by most hubs are described next.

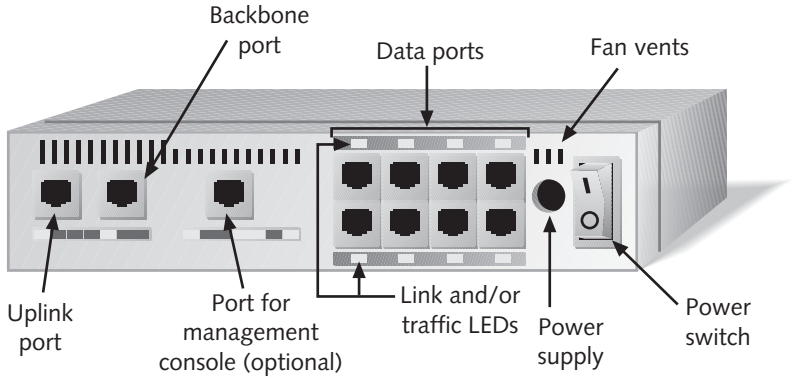


Figure 6-17 Detailed diagram of a hub

- *Ports*—Receptacles where patch cables connect workstations or other devices to the hub. The type of receptacle (RJ-45 versus BNC, for example) will depend on your network technology. The number of ports on a hub generally ranges from 4 to 24, but can be higher. This number does not include the uplink port, described below.
- *Uplink port*—The receptacle used to connect one hub to another hub in a daisy-chain or hierarchical fashion. An uplink port may look like any other port, but it should be used only to interconnect hubs.
- *Port for management console*—A receptacle used to connect some type of display, or console (such as a laptop PC), that enables you to view the hub's management information, such as the traffic load or number of collisions. Not all hubs provide management information, so not all have a management console port.
- *Backbone port*—The receptacle used to connect a hub to the network's backbone.
- *Link LED*—The light on a port that indicates whether it is in use. If a connection is live, this light should be solid green. If no connection exists, the light will be off. If you think that the connection is live but the light is not on, you need to check connections, transmission speed settings, and power supplies for both the network adapter and the hub.
- *Traffic (transmit or receive) LED*—The light on a port that indicates that traffic is passing through the port. Under normal data traffic situations, this light should blink green. Some hubs include separate LEDs for the transmission and receipt of data; others do not even have traffic LEDs for their ports. If they exist, traffic LEDs are normally found adjacent to link LEDs beside each data port.
- *Collision LED (Ethernet hubs only)*—The light that roughly indicates collisions by blinking. The faster the light blinks, the more collisions that are occurring on the network. The hub may include one collision LED for the entire hub or individual lights for each port. If this light is continuously lit, a node is experiencing dire connectivity or traffic problems and may need to be disconnected. Because only Ethernet hubs have collision LEDs, Figure 6-17 does not show one.

- *Power supply*—The device that provides power to the hub. Every hub has its own power supply (for this reason, you will want to connect critical hubs to a UPS, as explained in Chapter 14). Every hub also has its own power-on light. If the power-on light is not lit, the hub has lost power. The power light is normally found on the front of a hub, and so is not shown in Figure 6-17.
- *Ventilation fan*—A device used to cool a device's internal electronics. Hubs, like other electronic devices, generate heat. To function properly, most hubs must cool their processors, components, and circuitry with a ventilation fan (although very small hubs may not require a ventilation fan). When installing, you should be careful not to block or cover the air-intake vents.

Placement of hubs in a network design can vary. The simplest structure would employ a standalone workgroup hub that is connected to another connectivity device such as a switch or router. Most networks use several hubs to serve different workgroups, thereby benefiting from not having a single point of failure and possibly having switching and data management abilities. Figure 6-18 indicates how hubs may fit into the overall design of a network.

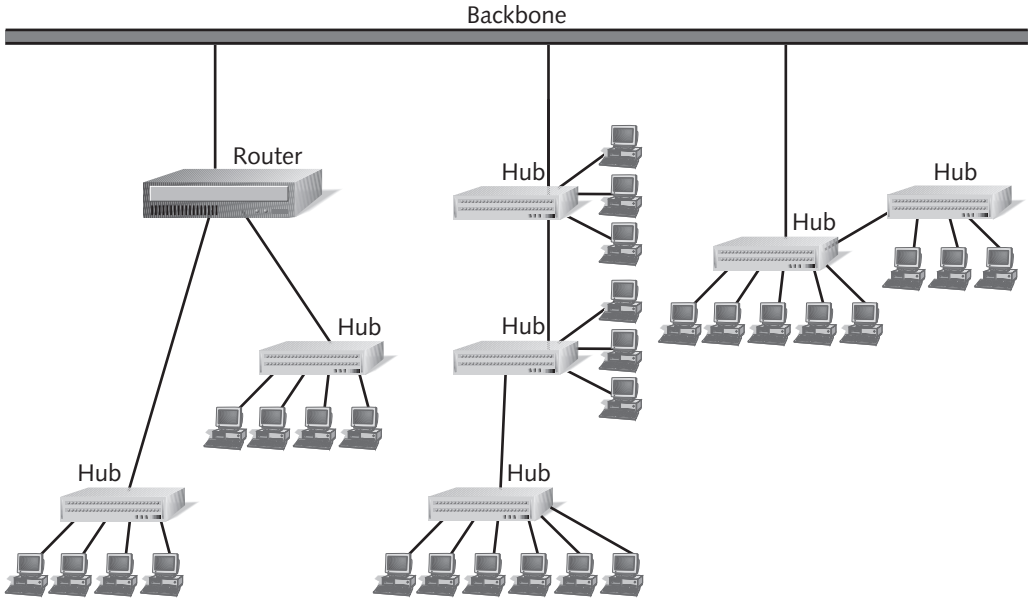


Figure 6-18 Hubs in a network design

Many hubs—known as **passive hubs**—do nothing but repeat signals. Like network adapters, however, some hubs possess internal processing capabilities. For example, they may permit remote management, filter data, or provide diagnostic information about the network. Hubs that can perform any of these functions are known as **intelligent hubs**.

Technological advances are making hubs more capable and more vital in network management. The following sections introduce the different types of hubs, their functions, advantages, and disadvantages. Hubs represent a significant element in network design, configuration, and troubleshooting. To prepare for the Net+ certification exam, you should pay close attention to the material in the following sections.

Standalone Hubs

Standalone hubs, as their name implies, are hubs that serve a group of computers that are isolated from the rest of the network. A standalone hub may be connected to another hub by a coaxial, fiber-optic, or twisted-pair cable; however, they are typically not connected in a hierarchical or daisy-chain fashion. Standalone hubs are best suited to small, independent departments, home offices, or test lab environments. They can be passive or intelligent, and they are simple to install and connect for a small group of users.

Standalone hubs do not follow one design, nor do they contain a standard number of ports (though they usually contain 4, 8, 12, or 24 ports). A small, standalone hub that contains only four ports (primarily used for a small or home office) may be called a "hubby," "hublet," or a "minihub." On the other hand, standalone hubs can provide as many as 200 connection ports. The disadvantage to using a single hub for so many connections is that you introduce a single point of failure on the network. A **single point of failure** is a device or connection on a network that, were it to fail, could cause the entire network to stop functioning. In general, a large network would include multiple hubs (or other connectivity devices). Figure 6-19 depicts some standalone hubs.

Figure 6-19 Standalone hubs

Stackable Hubs

Stackable hubs resemble standalone hubs, but they are physically designed to be linked with other hubs in a single telecommunications closet. Stackable hubs linked together logically represent one large hub to the network. A great benefit to using stackable hubs is that your network or workgroup does not depend on a single hub, which could present a single point of failure.

Models vary in the maximum number that can be stacked. For instance, some hub manufacturers restrict the number of their stacked hubs to five; others can be stacked eight units high.

Although many stackable hubs include Ethernet uplink ports, some use a proprietary high-speed cabling system to link the hubs together for better interhub performance. This setup often creates incompatibilities between the bus cabling of different product lines, even when those products come from the same manufacturer. Hubs that use standard Ethernet uplink ports can usually be interconnected with components of other product lines. As a general rule, although stacked hubs do not have to be made by the same manufacturer to work together properly, it is always preferable to interconnect hardware that is known to be compatible right out of the box.

Like standalone hubs, stackable hubs may support a number of different media connectors and transmission speeds and may come with or without special processing features. The number of ports they provide also varies, although you will most often see

6, 12, or 24 ports on a stackable hub. Figure 6-20 depicts a variety of stackable hubs, and Figure 6-21 shows a rack-mounted stackable hub system, such as you might find in a telecommunications closet.

Figure 6-20 Stackable hubs

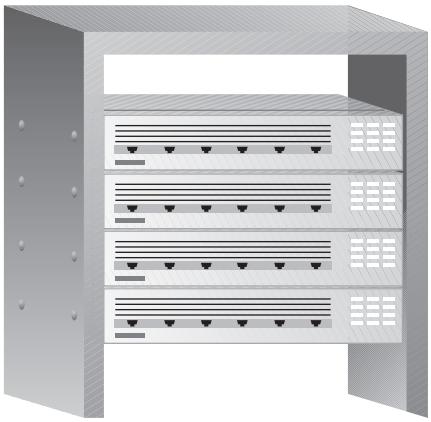


Figure 6-21 Rack-mounted stackable hubs

Modular Hubs

Modular hubs provide a number of interface options within one chassis, making them more flexible than either stackable or standalone hubs. Similar to a PC, a modular hub contains a system board and slots into which you can insert different adapters. These

adapters may connect the modular hub to other types of hubs, routers, WAN links, or Token Ring or Ethernet network backbones. They may also connect the modular hub to management workstations or redundant (extra) components, such as a second power supply. Because you can attach redundant components to modular hubs, they offer the highest reliability of any type of hub. Another benefit to modular hubs is that they allow for a network's future growth by providing expansion slots for additional devices. In addition, they can accommodate many types of devices. In other words, you can customize a modular hub to your network's needs. On the downside, modular hubs are the most expensive type of hub, and for a small network they may be overkill. Modular hubs are nearly always intelligent hubs.

Intelligent Hubs

Earlier in this chapter, you learned that an intelligent hub can process data, monitor traffic, and provide troubleshooting information, among other things. Intelligent hubs are also called **managed hubs**, because they can be managed from anywhere on the network. Remember that standalone, stackable, or modular hubs may all have processing capabilities and, therefore, be considered intelligent.

The advantage of intelligent hubs derives from their ability to analyze data. A network administrator can store the information generated by intelligent hubs in a MIB. A **MIB (management information base)** is a collection of data used by management programs (which may be part of the network operating system or third-party programs) to analyze network performance and problems. MIBs are typically used by programs that generate data via the SNMP protocol. Novell's ManageWise is one example of a program that relies on MIBs. From such a program, the network administrator can view the network layout in graphical form, disconnect problem nodes, set alarms to go off when certain events occur, identify nodes that may be generating unnecessary traffic, or find out information (such as IP addresses) about remote nodes. Using this tool, the network administrator can also track historical data about network traffic patterns—for example, to determine where greater bandwidth is needed.

Although you might be tempted to assume that intelligent hubs are your best solution in every situation, they have their disadvantages. For example, an intelligent hub will report every time a port detects a lost connection. In fact, lost connections happen hundreds of times each day—when a formerly connected workstation is restarted, for example. This event, its trivial nature notwithstanding, is recorded in the MIB, along with hundreds of other inconsequential events. When the MIB includes so many inconsequential events, network administrators may find it difficult to determine which errors are critical and which can be ignored. In addition, intelligent hubs are significantly more expensive than passive hubs. For a routine networking environment with limited staff, intelligent hubs might be more trouble than they are worth.

Installing a Hub

As with network adapters, the best way to ensure that you install a hub properly is to follow the manufacturer's guidelines. Most of the time, hubs are simple to install—arguably even simpler than connecting workstations to the network, because they require very little configuration.

First, plug the hub in and turn it on. Make sure that the hub's power light goes on. Most hubs will perform self-tests when turned on, and blinking lights will indicate that these tests are in progress. When the tests are completed (as indicated by a steady, lit power light on most hubs), attach the hub to the network by connecting a patch cable from it to the backbone or to an intermediate switch or router. Next, connect patch cables from the patch panel or workstations to the hub's receptacles, as shown in Figure 6-22. Once the workstation connects to the network through the newly installed hub, check to verify that the link and traffic lights act as they should, according to the hub's documentation.

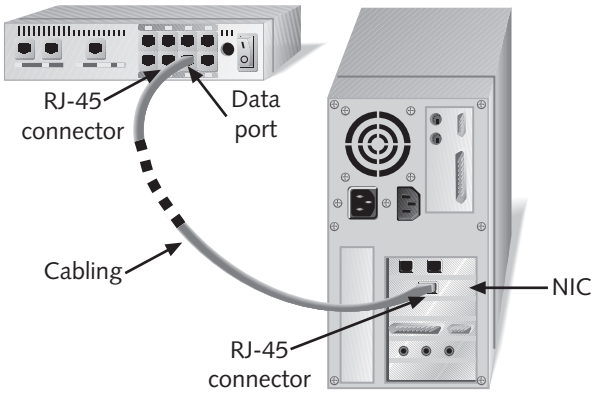


Figure 6-22 Connecting a workstation to a hub

Unless you are using a small, inexpensive hub, you will probably need to configure the hub's firmware and, in the case of intelligent hubs, its software as well. For example, you will need to assign an IP address to the hub. Refer to the instructions that came with your hub to find out how to configure its firmware and software.

If you are installing a stackable hub or a rack-mounted hub, you will need to use the screws and clamps that came with the hub to secure it to the rack or connect it to the other hubs. In the case of a stackable hub, you may need to connect it with its proprietary cabling or through its uplink port. Again, the best approach is to read the instructions that came with the hub.

Choosing the Right Hub

Any one of thousands of hubs might work on your network. So how do you decide which is right for you? First, narrow your list of options to hubs that match your network's logical topology, transmission speed, and media type. Then examine the following list of variables and decide which enhancements are necessary for your network and how much you can afford.

- *Performance*—If performance is your concern, you may want to use switches, rather than hubs, to subdivide a current LAN segment into several, smaller segments. You may also want to upgrade part of your network to a faster transmission technology (for example, from 10BaseT to 100BaseTX). To support this transition, you may need a hub that can handle traffic at *either* 10 Mbps or 100 Mbps. Because of the way in which hubs work, you should avoid mixing hubs that can handle only speeds of 10 Mbps with hubs that can handle speeds of 100 Mbps, because all 100 Mbps devices will be slowed down by the presence of even a single 10-Mbps device. Switches (discussed later in this chapter) do support the mixing of speeds.
- *Cost*—If your budget is tight and your environment does not demand the flexibility, reliability, or security of more sophisticated hubs, a passive standalone hub or a few passive stackable hubs might be your answer. If you have unlimited dollars to spend and need a hub with more features, you might consider an intelligent hub.
- *Size and growth*—You need to determine how many devices will connect to each hub in each telecommunications closet. If one segment consists of only 10 connections now but you know its size will double in six months, purchase a hub with at least 24 ports. (You must balance the number of hubs with the number of points of failure you are willing to risk on the network.)
- *Security*—If your network carries sensitive data, you should probably consider using more sophisticated connectivity equipment such as switches, routers, or firewalls.
- *Management benefits*—If you manage a huge enterprise-wide network containing many different types of devices and potential problems, you will want to purchase an intelligent hub, which is capable of providing management information to your network management program. This purchase will require more planning and technical expertise than other types of hubs.
- *Reliability*—If your network cannot tolerate any downtime, consider purchasing a modular hub with redundant power supplies and possibly redundant connections to the backbone as well.

As with network adapters, the hub manufacturer's documentation can vary.

BRIDGES

Bridges are devices that look like repeaters, in that they have a single input and a single output port, as shown in Figure 6-23. They differ from repeaters in that they can interpret the data they retransmit. Bridging occurs at the Data Link layer of the OSI Model; as you will recall from Chapter 3, this layer encompasses flow control, error handling, and physical addressing. Bridges analyze incoming frames and make decisions about how to direct them to their destination. Specifically, they read the destination (MAC) address information and decide whether to forward (retransmit) the packet to another segment on the network or, if the destination address belongs to the same segment as the source address, filter (discard) it. As nodes transmit data through the bridge, the bridge establishes a **filtering database** (also known as a **forwarding table**) of known MAC addresses and their locations on the network. The bridge uses its filtering database to determine whether a packet should be forwarded or filtered, as illustrated in Figure 6-24.

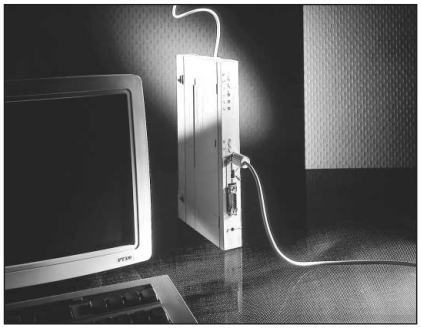


Figure 6-23 A bridge

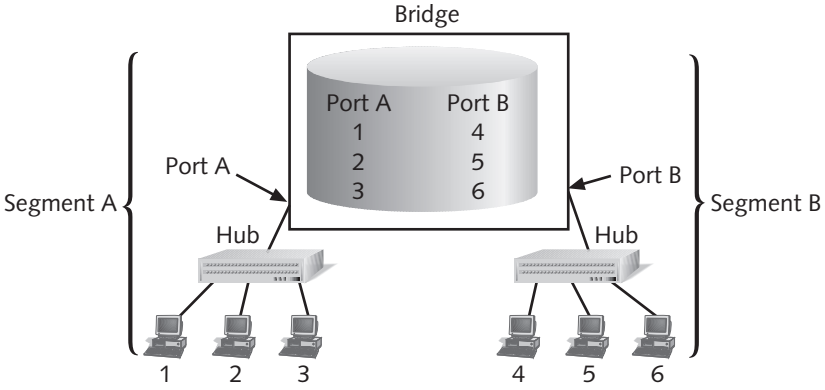


Figure 6-24 A bridge's use of a filtering database

Using Figure 6-24 as an example, imagine that you sit at workstation 1 on segment A of the LAN, and your colleague Abby sits at workstation 2 on segment A. When you attempt to send data to Abby's computer, your transmission will go through your segment's hub and then to the bridge. The bridge will read the MAC address of Abby's computer. It will then search its filtering database to determine whether that MAC address belongs to the same segment you're on or whether it belongs on a different segment. The bridge can determine only that the MAC address of Abby's workstation is associated with its port A. If the MAC address belongs to a different segment, the bridge forwards the data to that segment, whose corresponding port identity is also in the filtering database. In this case, however, your workstation and Abby's workstation reside on the same LAN segment, so the data would be filtered (that is ignored) and your message would be delivered to Abby's workstation through segment A's hub.

Conversely, if you wanted to send data to your supervisor's computer, which is workstation 5 in Figure 6-24, your transmission would first pass through segment A's hub and then on to the bridge. The bridge would read the MAC address for your supervisor's machine (the destination address in your data stream) and search for the port associated with that machine. In this case, the bridge would recognize workstation 5 as being connected to port B, and it would forward the data to that port. Subsequently, the segment B hub would ensure delivery of the data to your supervisor's computer.

After you install a new bridge, it will use one of several methods to learn about the network and discover where the destination address for each packet it handles resides. Once it discovers this information, it will record the destination node's MAC address and its associated port in its filtering database. Over time, it will discover all nodes on the network and construct database entries for each.

Because bridges cannot interpret higher-level data, such as Network layer information, they do not distinguish between different protocols. They can forward frames from AppleTalk, TCP/IP, IPX/SPX, and NetBIOS with equal speed and accuracy. This flexibility is a great advantage. Because they are protocol-ignorant, bridges can move data more rapidly than traditional routers, for example, which do care about protocol information (as you will learn later in this chapter). On the other hand, bridges take longer to transmit data than either repeaters or hubs, because bridges actually analyze each packet, while hubs do not.

Bridges may follow one of several types of methods for forwarding or filtering packets. A discussion of each of these methods is beyond the scope of this book, but you should at least be aware of the most popular options. The method used on many Ethernet networks is called **transparent bridging**. In transparent bridging a bridge begins polling a network to learn about its physical topology as soon as it is installed. When a bridge receives a packet from an unknown source, it adds the location of that source to its filtering database. Over time, it compiles database entries for each network node, and forwards packets according to the examples discussed earlier in this section. The disadvantage of transparent bridging is that, on large LANs containing multiple

bridges, each bridge may recognize a different path to a particular network node. When this is the case, data that must traverse more than one bridge to get to its destination may get bounced back and forth among the bridges. This causes packets to travel endlessly over the network, never reaching their destination. To avoid this problem, networks may use the spanning tree algorithm. The **spanning tree algorithm** is a routine that can detect circular traffic patterns and modify the way multiple bridges work together, in order to avoid such patterns.

The bridging method used on most Token Ring networks is called **source-route bridging**. In source-route bridging, a bridge polls the network to determine what path is the best way for a packet to get from point A to point B. The bridge then adds this information to the data packet. Because forwarding information becomes part of the data, source-route bridging is not susceptible to the circular traffic problems that transparent bridging may suffer. This makes source-route bridging especially well suited to WANs, where multiple bridges and long routes are common.

When bridges were first introduced in the early 1980s, they were designed to forward packets between homogenous networks. Since then, however, bridges have evolved to handle data transfer between different types of networks. A method of bridging that can connect networks that use different logical topologies is called **translational bridging**. In translational bridging, the bridge not only forwards packets, but also translates packets between one logical topology and another. Translational bridging may be used, for example, to connect a Token Ring network to an Ethernet network, or a FDDI network to an Ethernet network.

Bridges have also enjoyed advances in their filtering techniques and transmission speed. Even though sophisticated routers and switches have replaced many network bridges, bridges may still be adequate and appropriate in some situations. The inclusion of a bridge on a network enhances the network performance by filtering traffic directed to the various nodes; the nodes therefore spend less time and resources listening for data that may or may not be destined for them. Also, a bridge can detect and discard flawed packets that may create congestion on the network. Perhaps most importantly, bridges extend the maximum distance of a network beyond its previous limits.

Standalone bridges became popular in the 1980s and early 1990s, but they have largely been made obsolete by advanced switching and routing technology. In general, you will rarely work with bridges as standalone devices. Nevertheless, understanding the concept of bridging is essential to understanding how switches work. You will learn more about switches in the next section.

SWITCHES

In recent years, advances in connectivity hardware have blurred the strict distinctions between hubs, switches, routers, and bridges. **Switches** subdivide a network into smaller logical pieces. Unlike hubs, which operate at Layer 1 of the OSI Model, they operate at

the Data Link layer (Layer 2) of the OSI Model and can interpret MAC address information. In this sense, switches resemble bridges. In fact, they can be described as multiport bridges. Figure 6-25 illustrates several switches.

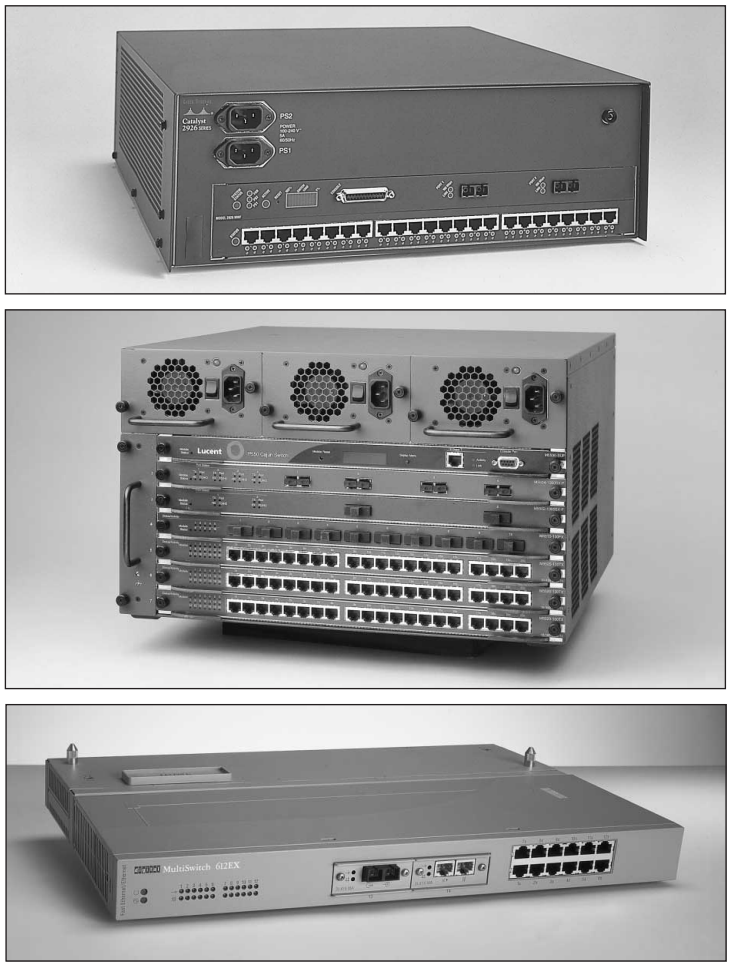


Figure 6-25 Examples of LAN switches

Because they have multiple ports, switches can make better use of limited bandwidth and prove more cost-efficient than bridges. Each port on the switch acts like a bridge, and each device connected to a switch effectively receives its own dedicated channel. In other words, a switch can turn a shared channel into several channels.

From the Ethernet perspective, each dedicated channel represents a collision domain. Recall from Chapter 5 that a collision domain is a logically or physically distinct Ethernet network segment on which all participating devices must detect and accommodate data

collisions. Because a switch limits the number of devices in a collision domain, it limits the potential for collisions.

Switches have historically been used to replace hubs and ease traffic congestion in LAN workgroups. Introducing a switch on a congested segment is only a temporary solution, however, and arguably not the best use of such a device. More recently, network managers have replaced backbone routers with switches, and switch sales are, therefore, booming.

The inclusion of switches on a network backbone provides at least two advantages. First, switches are generally very secure because they isolate one device's traffic from other devices' traffic. Second, switches provide separate channels for (potentially) every device. As a result, applications that transfer a large amount of traffic and are sensitive to time delays, such as videoconferencing applications, can make full use of the network's capacity.

Switches have their disadvantages, too. Although they contain buffers to hold incoming data and accommodate bursts of traffic, they can become overwhelmed by continuous, heavy traffic. In that event, the switch cannot prevent data loss. On a shared environment, where many nodes share the same data channel, devices can compensate for collisions; on a fully switched network, where every node uses its own port on the switch and therefore has a separate data channel, devices cannot detect collisions. Also, although higher-layer protocols, such as TCP, will detect the loss and respond with a timeout, others, such as UDP, will not. For packets using such protocols, the number of collisions will mount up, and eventually all network traffic will grind to a halt. For this reason, you should plan placement of switches carefully to match backbone capacity and traffic patterns.

Switches can be classified into a few different categories. One type, a LAN switch, functions on a local area network. LAN switches can be designed for Ethernet or Token Ring networks, although Ethernet LAN switches are more common. LAN switches also differ in the method of switching they use—namely, cut-through mode or store and forward mode. These methods of switching on a LAN are discussed in the next two sections.

Keep in mind that the term *switch* is also sometimes applied to WAN and access server devices. You will learn more about WAN and remote connectivity in Chapter 7.

Cut-Through Mode

A switch running in **cut-through mode** will read a frame's header and decide where to forward the data before it receives the entire packet. Recall from Chapter 5 that the first 14 bytes of a frame constitute its header, which contains the destination MAC address. This information is sufficient for the switch to determine which port should get the frame and begin transmitting the frame (without bothering to hold the data and check its accuracy).

What if the frame becomes corrupt? Because the cut-through mode does not allow the switch to read the frame check sequence before it begins transmitting, it can't verify data integrity in that way. On the other hand, cut-through switches can detect **runts**, or packet fragments. Upon detecting a runt, the switch will wait to transmit that packet until it determines its integrity. It's important to remember, however, that runts are only one type of data flaw. Cut-through switches *cannot* detect corrupt packets; indeed, they may increase the number of errors found on the network by propagating flawed packets.

The most significant advantage of the cut-through mode is its speed. Because it does not stop to read the entire data packet, a cut-through switch can forward information much more rapidly than a store and forward switch can (as described in the next section). The time-saving advantages to cut-through switching become insignificant, however, if the switch is flooded with traffic. In this case, the cut-through switch must buffer (or temporarily hold) data, just like a store and forward switch. Cut-through switches are best suited to small workgroups where speed is important and the relatively low number of devices minimizes the potential for errors.

Store and Forward Mode

In **store and forward mode**, a switch reads the entire data frame into its memory and checks it for accuracy before transmitting the information. Although this method is more time-consuming than the cut-through method, it allows store and forward switches to transmit data more accurately. Store and forward mode switches are more appropriate for larger LAN environments because they do not propagate data errors. In contrast, cut-through mode switches do forward errors, so they may contribute to network congestion if a particular segment is experiencing a number of collisions. In large environments, a failure to check for errors can result in problematic traffic congestion.

Store and forward switches can also transfer data between segments running different transmission speeds. For example, a high-speed network printer that serves 50 students could be attached to a 100-Mbps port on the switch, thereby allowing all of the student workstations to connect to 10-Mbps ports on the same switch. With this scheme, the printer can quickly service multiple jobs. This characteristic makes store and forward mode switches preferable in mixed-speed environments.

Using Switches to Create VLANs

In addition to improving bandwidth usage, switches can create **virtual local area networks (VLANs)**, a logically separate network within a network, by grouping a number of ports into a broadcast domain. A **broadcast domain** is a combination of ports that make up a Layer 2 segment and must be connected by a Layer 3 device, such as a router or Layer 3 switch. The ports do not have to reside on the same switch or even on the same network segment. A VLAN can include servers, workstations, printers, routers, or any other network device you can connect to a switch. Figure 6-26 illustrates a simple VLAN design. Note, however, that one great advantage of VLANs is their ability to link geographically distant users and create small workgroups from large LANs.

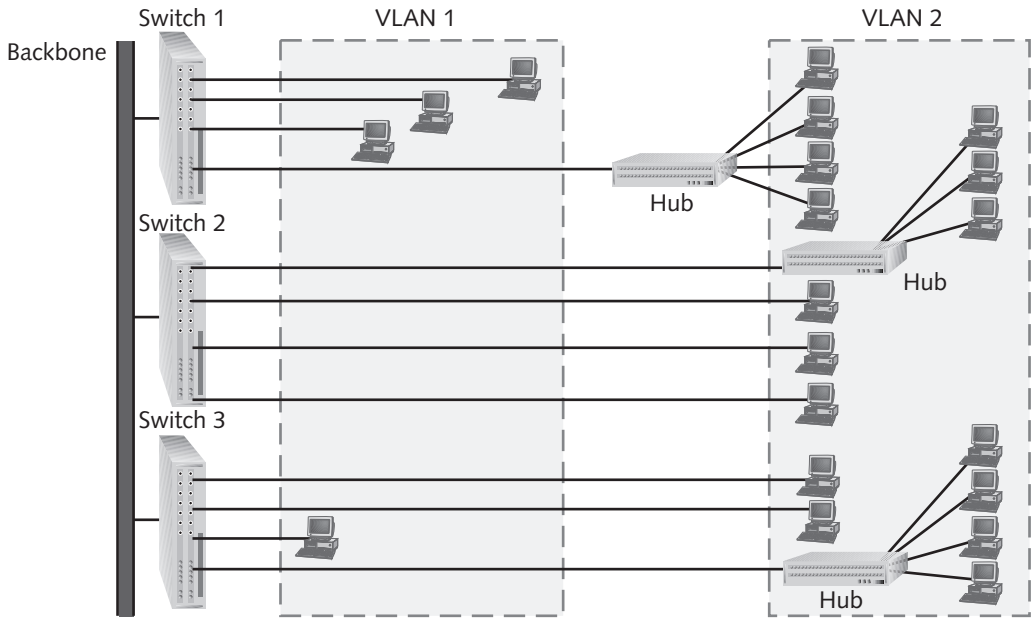


Figure 6-26 A simple VLAN design

To create a VLAN, you must configure the switch properly. In addition to identifying the ports that belong to each logical network, you can specify security parameters, filtering instructions (if the switch should not forward any frames from a certain segment, for example), performance requirements for certain users, and network management options. Clearly, switches are very flexible devices.

Describing the variety of ways in which VLANs may be implemented is beyond the scope of this book. If you are charged with designing a network or installing switches, however, you should research VLANs further. Some trade publications (and many switch manufacturers) have touted VLANs as the most advanced approach to networking and the wave of the future.

In setting up a VLAN, you are not merely including a certain group of nodes—you are also excluding another group. As a result, you can potentially cut a group off from the rest of the network. VLAN implementation requires careful planning to ensure that all the groups of users who need to communicate can do so after the VLAN is in operation.

Higher-Layer Switches

Earlier in this chapter, you learned that switches operate in Layer 2 (Data Link layer) of the OSI Model, routers operate in Layer 3, and hubs operate in Layer 1. You also learned that the distinctions between hubs, bridges, switches, and routers are blurring. This melding of categories will become more pronounced as switch technology advances. Indeed, manu-

facturers are already producing switches that can operate at Layer 3 (Network layer) and Layer 4 (Transport layer), making them act more like routers. A switch capable of interpreting Layer 3 data is called a **Layer 3 switch**. Similarly, a switch capable of interpreting Layer 4 data is called a **Layer 4 switch**. These higher-layer switches may also be called **routing switches** or **application switches**.

Among other things, the ability to interpret higher-layer data enables switches to perform advanced filtering, statistics keeping, and security functions. Layer 3 and Layer 4 switches may also transmit data more rapidly than a router and will probably remain easier to install and configure than routers. In general, these switches aren't as fully featured as routers. For example, they typically cannot translate between Token Ring and Ethernet networks, encapsulate protocols, or prioritize traffic. These critical differences make switches inappropriate for specific connectivity needs. In other words, if you needed to connect a 10BaseT Ethernet LAN with a 100BaseT Ethernet LAN, a switch would be adequate. If you wanted to connect a Token Ring LAN with an Ethernet LAN, you would want to use a router.

As with other connectivity devices, the features of these Layer 3 and Layer 4 switches vary widely depending on the manufacturer and the price. (This variability is exacerbated by the fact that key players in the networking trade have not agreed on standards for these switches.) Higher-layer switches can cost three times more than Layer 2 switches, and network administrators are only beginning to try them. In general, higher-layer switches are yet another technology you will need to watch closely.

ROUTERS

A **router** is a multiport connectivity device that can integrate LANs and WANs running at different transmission speeds and using a variety of protocols. Routers operate at the Network layer (Layer 3) of the OSI Model. Recall from Chapter 2 that the Network layer directs data from one segment or type of network to another. Historically, routers have been slower than switches or bridges because they pay attention to information in Layers 3 and higher, such as protocols and logical addresses. Consequently, unlike bridges and Layer 2 switches, routers are protocol-dependent. They must be designed or configured to recognize a certain protocol before they can forward data transmitted using that protocol.

As is the case with bridges, traditional standalone LAN routers are being replaced by Layer 3 switches that support the routing functions. The concept of routing remains extremely important, however, and everything described in the remainder of this section also applies to Layer 3 switches. Standalone routers are still the technology of choice for connecting remote offices using WAN technology.

Router Features and Functions

A router's strength lies in its intelligence. Not only can routers only keep track of the locations of certain nodes on the network, as switches can, but they can also determine the

shortest, fastest path between two nodes. For this reason, and because they can connect dissimilar network types, routers are powerful, indispensable devices on large LANs and WANs. The Internet, for example, relies on a multitude of routers across the world.

As noted in Chapter 3, some protocols are not routable. Routable protocols include TCP/IP, IPX/SPX, and AppleTalk. Because NetBEUI and SNA are not routable, for example, networks that run these protocols cannot use routers. On the other hand, some routers provide advanced support for Layer 2 bridging that far exceeds what a bridge or switch can accomplish. These bridge-routers (or brouters) are discussed later in this chapter.

A typical router has an internal processor, its own memory and power supply, input and output jacks for different types of network connectors (depending on the network type), and, usually, a management console interface, as shown in Figure 6-27. High-powered, multiprotocol routers may have several slot bays to accommodate multiple network interfaces (RJ-45, BNC, FDDI, and so on). A router with multiple slots that can hold different interface cards or other devices is called a **modular router**.

Figure 6-27 Routers

A router is a very flexible device. Although any one can be specialized for a variety of tasks, all routers can do the following: connect dissimilar networks, interpret Layer 3 information, determine the best path for data to follow from point A to point B, and reroute traffic if a primary path is down but another path is available. In addition to performing these basic functions, routers may perform any of the following optional functions:

- Filter out broadcast transmissions to alleviate network congestion
- Prevent certain types of traffic from getting to a network, enabling customized segregation and security
- Support simultaneous local and remote connectivity
- Provide high network fault tolerance through redundant components such as power supplies or network interfaces
- Monitor network traffic and report statistics to a MIB
- Diagnose internal or other connectivity problems and trigger alarms

In addition, routers may use one of two methods for directing data on the network: static or dynamic routing. **Static routing** is a technique in which a network administrator programs a router to use specific paths between nodes. Since it does not account for occasional network congestion, failed connections, or device moves, static routing is not optimal. If a router or a segment connected to a router is moved, the network administrator must reprogram the static router's tables. The fact that static routing requires human intervention makes it less efficient and accurate than dynamic routing. **Dynamic routing**, on the other hand, automatically calculates the best path between two nodes and accumulates this information in a routing table. If congestion or failures affect the network, a router using dynamic routing can detect the problems and reroute data through a different path. Most modern networks primarily use dynamic routing, but may include some static routing to indicate a router of last resort, the router that accepts all unroutable packets.

Because of their customizability, routers are not simple devices to install. Typically, a technician or engineer must be very familiar with routing technology to figure out how to place and configure a router to best advantage. Figure 6-28 gives you some idea of how routers fit into a LAN environment, although this example is oversimplified. If you plan to specialize in network design or router configuration, you should research router technology further. You might begin with Cisco System's online documentation at *www.cisco.com/univercd/home/home.htm*. Cisco Systems currently provides the majority of networking routers installed in the world.

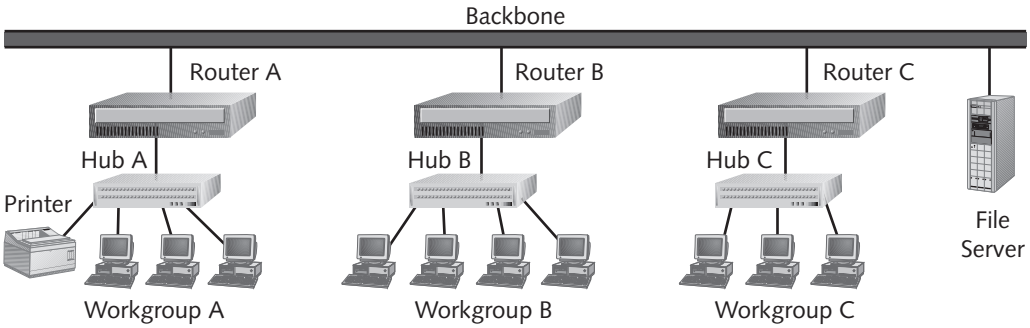


Figure 6-28 The placement of routers on a LAN

In the setup depicted in Figure 6-28, if a workstation in workgroup C wanted to print to a networked printer in workgroup A, it would create a transmission containing the address of the workgroup A printer. Then it would send its packets to hub C. Hub C would simply retransmit the signal to router C. When router C received the transmission, it would temporarily store the packets as it read the Layer 3 information. Upon determining that the packets were destined for a printer in workgroup A, router C would then decide the best way to get the data to the workgroup A printer. In this example, it might send the data directly to router A. Before it forwards the packet, however, router C would increment (increase) the number of hops tallied in the packet. A **hop** is the term used in networking to describe each trip data take from one connectivity device to another. (Usually, the term is used in the context of routing.) For example, a trip from a workstation in Workgroup A to Hub A would constitute one hop, and a trip from Hub A to Router A would constitute another hop. Each time a packet passes through a router, it has made a hop. Packets can only take a certain number of hops before they are discarded. (Recall the network distance limitations you learned about in Chapter 4.)

After it incremented the number of hops tallied in the packet, router C would forward the data to router A. Router A would increment the packet's hop count, read the packet's destination address and forward it to hub A, which would then broadcast the transmission to workgroup A until the printer picked it up.

Routing Protocols: RIP, OSPF, EIGRP, and BGP

Finding the best route for data to take across the network is one of the most valued and sophisticated functions performed by a router. The term **best path** refers to the most efficient route from one node on a network to another. The best path in a particular situation depends on the number of hops between nodes, the current network activity, the unavailable links, the network transmission speed, and the topology. To determine the best path, routers communicate with each other through **routing protocols**. Keep in mind that routing protocols are *not* the same as routable protocols, such as TCP/IP or IPX/SPX, although routing protocols may piggyback on top of routable protocols. Routing protocols are used only to collect data about current

network status and contribute to the selection of the best paths. From these data, routers create routing tables for use with future packet forwarding.

In addition to its ability to find the best path, a routing protocol can be characterized according to its **convergence time**, the time it takes for a router to recognize a best path in the event of a change or network outage. Its **bandwidth overhead**, the burden placed on the underlying network to support the routing protocol, is also a distinguishing feature.

Although you do not need to know precisely how routing protocols work in order to qualify for the Network+ certification, you should be familiar with the most common routing protocols: RIP, OSPF, EIGRP, and BGP. (Several more routing protocols exist, but are not widely used.) These four common routing protocols are described below.

- *RIP (Routing Information Protocol) for IP and IPX*—The oldest routing protocol, RIP, which is still widely used, factors in only the number of hops between nodes when determining a path from one point to another. It does not consider network congestion or link speed, for example. Routers using RIP broadcast their routing tables every 30 seconds to other routers, whether or not the tables have changed. This broadcasting creates excessive network traffic, especially if a large number of routes exist. If the routing tables change, it may take several minutes before the new information propagates to routers at the far reaches of the network; thus the convergence time for RIP is poor. RIP is limited to interpreting a maximum of 16 hops, so it does not work well in very large network environments where data may have to travel through more than 16 routers to reach their destination (for example, on the Internet). Also, compared with other routing protocols, RIP is slower and less secure.
- *OSPF (Open Shortest Path First) for IP*—This routing protocol makes up for some of the limitations of RIP and can coexist with RIP on a network. OSPF uses a more complex algorithm for determining best paths. Under optimal network conditions, the best path is the most direct path between two points. If excessive traffic levels or an outage preclude data from following the most direct path, a router may determine that the most efficient path actually goes through additional routers. Each router maintains a database of the other routers' links, and if notice is received indicating the failure of a given link, the router can rapidly compute an alternate path. This approach requires more memory and CPU power on the routers, but it keeps network bandwidth to a minimum and provides a very fast convergence time, often invisible to the users. OSPF is the second most frequently supported protocol, after RIP.
- *EIGRP (Enhanced Interior Gateway Routing Protocol) for IP, IPX, and AppleTalk*—This routing protocol was developed in the mid-1980s by Cisco Systems. It has a fast convergence time and a low network overhead, and is easier to configure and less CPU-intensive than OSPF. EIGRP also offers the benefits of supporting multiple protocols and limiting unnecessary network traffic between routers. It accommodates very large and heterogeneous networks, but is only supported by Cisco routers.

- *BGP (Border Gateway Protocol) for IP*—BGP is the routing protocol of Internet backbones. The demands on routers created by Internet growth have driven the development of BGP, the most complex of the routing protocols. The developers of BGP had to contend with not only the prospect of 100,000 routes, but also the question of how to route traffic efficiently and fairly through the hundreds of Internet backbones.

Brouters and Routing Switches

By now it should not surprise you that routers, too, can act like other devices. The networking industry has adopted the term **bridge router**, or **brouter**, to describe routers that take on some characteristics of bridges. The advantage of crossing a router with a bridge is that you can forward nonroutable protocols, such as NetBEUI, plus connect multiple network types through one device. A bridge router offers support at both Layers 2 and 3 of the OSI Model. It intelligently handles any packets that contain Layer 3 addressing information and simply forwards the rest.

Another router hybrid, a **routing switch**, combines a router and a switch. It can also interpret data from both Layers 2 and 3 of the OSI Model. (*Routing switch* is another term for the higher-layer switches covered earlier in this chapter.) A routing switch is not as fully featured as a true router, and therefore routing switches have not gained wide acceptance from networking professionals.

GATEWAYS

Gateways do not fall neatly into the networking hardware category. In broad terms, they are combinations of networking hardware and software that connect two dissimilar kinds of networks. Specifically, they may connect two systems that use different formatting, communications protocols, or architecture. Unlike the connectivity hardware discussed earlier in this chapter, gateways actually repackage information so that it can be read by another system. To accomplish this task, gateways must operate at multiple layers of the OSI Model. They must communicate with an application, establish and manage sessions, translate encoded data, and interpret logical and physical addressing data.

Gateways can reside on servers, microcomputers, or mainframes. They are more expensive than routers because of their vast capabilities and almost always application-specific. In addition, they transmit data much more slowly than bridges or routers because of the complex translations they conduct. Because they are slow, gateways have the potential to cause extreme network congestion. In certain situations, however, only a gateway will suffice.

During your networking career, you will most likely hear gateways discussed in the context of e-mail systems. Popular types of gateways, including e-mail gateways, are described below.

- *E-mail gateway*—A gateway that translates messages from one type of e-mail system to another. For example, an e-mail gateway would allow people who use Eudora e-mail to correspond with people who use GroupWise e-mail.
- *IBM host gateway*—A gateway that establishes and manages communication between a PC and an IBM mainframe computer.
- *Internet gateway*—A gateway that allows and manages access between LANs and the Internet. An Internet gateway can restrict the kind of access LAN users have to the Internet, and vice versa.
- *LAN gateway*—A gateway that allows segments of a LAN running different protocols or different network models to communicate with each other. A router, a single port on a router, or even a server may act as a LAN gateway. The LAN gateway category might also include remote access servers that allow dial-up connectivity to a LAN.

Chapter Summary

- Network interface cards (NICs) come in a variety of types depending on logical topology (Ethernet versus Token Ring), network transmission speed (for example, 10 Mbps versus 100 Mbps), connector interfaces (for example, BNC versus RJ-45), type of compatible system board or device, and manufacturer.
- For a desktop or tower PC, an expansion card network adapter is used. It must match the system's bus. A bus is the type of circuit used by the system board to transmit data to components. Network adapters may fit ISA, EISA, MCA, or PCI buses. New computers almost always use PCI buses.
- Network adapters may also be externally attached, through the PCMCIA, USB, or parallel port.
- In addition to network adapters that interface with network cabling, network adapters can be designed for wireless transmission. A wireless network adapter uses an antenna to exchange signals with the network. This type of connectivity suits environments where cabling cannot be installed or where roaming clients must be supported.
- Devices other than PCs, such as networked printers, use specialized network adapters. Printer network adapters also come in a variety of styles suited to different applications. By far, the most popular printer network adapter is Hewlett-Packard's JetDirect card.
- To install a NIC, you must physically attach it to the bus (or port), install the NIC device drivers, and configure its settings.
- On servers, you may need to install multiple network adapters. For the hardware installation, you can repeat the same installation process used for the first network adapter, choosing a different slot. The trick to using multiple network adapters lies in correctly configuring the software for each.

- Some older NICs require hardware adjustments to indicate different variables, such as IRQ or I/O address settings. They may use jumpers, small plastic pieces containing a metal bridge that closes a circuit between two pins on the expansion card, or DIP switches, small plastic toggle switches that can indicate an "on" or "off" position.
- Firmware combines hardware and software. The hardware component of firmware is an electrically erasable programmable read-only memory (EEPROM) chip that stores data established at the factory. This data can be changed by configuration software.
- An IRQ is the means by which a device can request attention from the CPU. IRQ numbers range from 0 to 15. The BIOS will attempt to assign free IRQ numbers to new devices. Typically, it will assign IRQ numbers 9,10, or 11, to network adapters. If conflicts occur, you must manually assign a device's IRQ number rather than accept the default suggested by the BIOS.
- Many IRQ numbers are preassigned to system devices. For example, a keyboard uses IRQ 1, COM1 and COM3 use IRQ 4, a floppy disk drive uses IRQ 6, LPT1 uses IRQ 7, the clock uses IRQ 8, and the math coprocessor uses IRQ 13.
- To change a network adapter's firmware, you will need a bootable floppy disk (DOS version 6.0 or higher) containing the configuration or the DOS install utility that shipped with the network adapter. To run the utility, you must start the computer with this floppy disk inserted.
- Repeaters are the connectivity devices that perform the regeneration of a digital signal. They belong to the Physical layer of the OSI Model; therefore, they do not have any means to interpret the data they are retransmitting.
- At its most primitive, a hub is a multiport repeater. A simple hub may contain multiple ports that can connect a group of computers in a peer-to-peer fashion, accepting and repeating signals from each node. A slightly more sophisticated hub may contain multiple ports for devices and one port that connects to a network's backbone. Hubs typically support a star or hybrid topology on an Ethernet network. On Token Ring networks, hubs are called Multistation Access Units (MAUs).
- Hubs that merely repeat signals are called passive hubs.
- Intelligent hubs are also called managed hubs, because they can be managed from anywhere on the network. A standalone, stackable, or modular hub may include processing capabilities and, therefore, be considered intelligent.
- A MIB (management information base) is a collection of data used by management programs (which may be part of the network operating system or a third-party program) to analyze network performance and problems.
- Bridges resemble repeaters in that they have a single input and a single output port, but they can interpret the data they retransmit. Bridging occurs at the Data Link layer of the OSI Model. Bridges read the destination (MAC) address information and decide whether to forward (retransmit) a packet to another segment on the

network or, if the destination address belongs to the same segment as the source address, filter (discard) it.

- As nodes transmit data through the bridge, the bridge establishes a filtering database of known MAC addresses and their locations on the network. The bridge uses its filtering database to determine whether a packet should be forwarded or filtered.
- Switches subdivide a network into smaller logical pieces. They operate at the Data Link layer (Layer 2) of the OSI Model and can interpret MAC address information. In this respect, switches resemble bridges.
- Switches are generally secure because they isolate one device's traffic from other devices' traffic. Because switches provide separate channels for (potentially) every device, they allow applications that transfer a large amount of traffic and that are sensitive to time delays, such as videoconferencing, to make full use of the network's capacity.
- A switch running in cut-through mode will read a frame's header and decide where to forward the data before it receives the entire packet.
- In store and forward mode, switches read the entire data frame into their memory and check it for accuracy before transmitting it. Although this method is more time-consuming than the cut-through method, it allows store and forward switches to transmit data more accurately.
- In addition to improving bandwidth usage, switches can create virtual local area networks (VLANs) by logically grouping several ports into a broadcast domain. The ports do not have to reside on the same switch or even on the same network segment.
- Manufacturers are producing switches that can operate at Layer 3 (Network layer) and Layer 4 (Transport layer) of the OSI Model, making them act more like routers. The ability to interpret higher-layer data enables switches to perform advanced filtering, statistics keeping, and security functions.
- A router is a multiport device that can connect dissimilar LANs and WANs running at different transmission speeds and using a variety of protocols. Routers operate at the Network layer (Layer 3) or higher of the OSI Model. Historically, routers have transmitted data more slowly than switches or bridges because they pay attention to Layer 3 information, such as protocols and logical addresses.
- Unlike bridges and traditional switches, routers are protocol-dependent. They must be designed or configured to recognize a certain protocol before they can forward data transmitted using that protocol.
- A typical router has an internal processor, its own memory and power supply, input and output jacks for different types of network connectors (depending on the network type), and, usually, a management console interface.
- Finding the best route for data to take across the network is an important router function. The best path will depend on the number of hops between nodes, the

current network activity, the unavailable links, the network transmission speed, and the topology. To determine the best path, routers communicate with each other through routing protocols.

- Static routing is a technique in which a network administrator programs a router to use specific paths between nodes.
- Dynamic routing automatically calculates the best path between two nodes and accumulates this information in a routing table. If congestion or failures affect the network, a router using dynamic routing can detect the problems and reroute data through a different path. Most modern networks primarily use dynamic routing.
- The networking industry has adopted the term "brouter" to describe routers that take on some of the characteristics of bridges. Crossing a router with a bridge allows you to forward data using nonroutable protocols, such as NetBEUI, and to connect multiple network types through one device. A brouter offers support at both Layers 2 and 3 of the OSI Model.
- Gateways are combinations of networking hardware and software that connect two dissimilar kinds of networks. Specifically, they may connect two systems that use different formatting, communications protocols, or architecture. To accomplish this task, they must operate at multiple layers of the OSI Model.
- Typically, gateways are used for one of four purposes: as an e-mail gateway, as an IBM host gateway, as an Internet gateway, or as a LAN gateway.

Key Terms

adapter card — See *expansion board*.

application switch — Another term for a Layer 3 or Layer 4 switch.

bandwidth overhead — The burden placed on the underlying network to support a routing protocol.

base I/O port — A setting that specifies, in hexadecimal notation, which area of memory will act as a channel for moving data between the network adapter and the CPU. Like its IRQ, a device's base I/O port cannot be used by any other device.

best path — The most efficient route from one node on a network to another. Under optimal network conditions, the best path is the most direct path between two points.

BIOS (basic input/output system) — Firmware attached to the system board that controls the computer's communication with its devices, among other things.

Border Gateway Protocol (BGP) — The routing protocol of Internet backbones. The router stress created by Internet growth has driven the development of BGP, the most complex of the routing protocols. The developers of BGP had to contend with the prospect of 100,000 routes as well as the goal of routing traffic efficiently and fairly through the hundreds of Internet backbones.

bridge — A device that looks like a repeater, in that it has a single input and a single output, but is different from a repeater in that it can interpret the data it retransmits.

bridge router (brouter) — A router capable of providing Layer 2 bridging functions.

broadcast domain — In a virtual local area network (VLAN), a combination of ports that make up a Layer 2 segment and must be connected by a Layer 3 device, such as a router or Layer 3 switch.

brouter — See *bridge router*.

bus — The type of circuit used by the system board to transmit data to components. Most new Pentium computers use buses capable of exchanging 32 or 64 bits of data. As the number of bits of data a bus handles increases, so too does the speed of the device attached to the bus.

CMOS (complementary metal oxide semiconductor) — Firmware on a PC's system board that enables you to change its devices' configurations.

collision domain — A portion of a LAN encompassing devices that may cause and detect collisions among their group. Bridges and switches can logically create multiple collision domains.

convergence time — The time it takes for a router to recognize a best path in the event of a change or network outage.

cut-through mode — A switching mode in which a switch reads a frame's header and decides where to forward the data before it receives the entire packet. Cut-through mode is faster, but less accurate, than the other switching method, store and forward mode.

daughter board — See *expansion board*.

daughter card — See *expansion board*.

device driver — Software that enables an attached device to communicate with the computer's operating system.

DIP (dual inline package) switch — A small plastic toggle switch on a circuit board that can be flipped to indicate either an "on" or "off" status, which translates into a parameter setting.

dynamic routing — A method of routing that automatically calculates the best path between two nodes and accumulates this information in a routing table. If congestion or failures affect the network, a router using dynamic routing can detect the problems and reroute data through a different path. Most modern networks primarily use dynamic routing.

electrically erasable programmable read-only memory (EEPROM) — A type of ROM that is found on a circuit board and whose configuration information can be erased and rewritten through electrical pulses.

Enhanced Interior Gateway Routing Protocol (EIGRP) — A routing protocol developed in the mid-1980s by Cisco Systems that has a fast convergence time and a low network overhead, but is easier to configure and less CPU-intensive than OSPF. EIGRP also offers the benefits of supporting multiple protocols and limiting unnecessary network traffic between routers.

expansion board — A circuit board used to connect a device to a computer's system board.

expansion card — See *expansion board*.

expansion slots — Openings on a computer's system board that contain multiple electrical contacts into which the expansion board can be inserted.

Extended Industry Standard Architecture (EISA) — A 32-bit bus that is compatible with older ISA devices (because it shares the same length and pin configuration as the ISA bus), but that uses an extra layer of pins (resulting in a deeper, two-layered slot connector) for a second 16 bits to achieve faster throughput. The EISA bus was introduced in the late 1980s to compete with IBM's MCA bus.

filtering database — A collection of data created and used by a bridge that correlates the MAC addresses of connected workstations with their locations. A filtering database is also known as a forwarding table.

firmware — A combination of hardware and software. The hardware component of firmware is a read-only memory (ROM) chip that stores data established at the factory and possibly changed by configuration programs that can write to ROM.

forwarding table — See *filtering database*.

gateway — A combination of networking hardware and software that connects two dissimilar kinds of networks. Gateways perform connectivity, session management, and data translation, so they must operate at multiple layers of the OSI Model.

hop — A term used in networking to describe each trip data take from one connectivity device to another.

hub — A multiport repeater containing multiple ports to interconnect multiple devices. Unless they are used on a peer-to-peer network, hubs also contain an uplink port, one port that connects to a network's backbone. Hubs regenerate digital signals.

Industry Standard Architecture (ISA) — The original PC bus, developed in the early 1980s to support an 8-bit and later 16-bit data transfer capability. Although an older technology, ISA buses are still used to connect serial devices, such as mice or modems, in new PCs.

intelligent hub — A hub that possesses processing capabilities and can therefore monitor network traffic, detect packet errors and collisions, poll connected devices for information, and send the data gathered to a management information base (MIB).

interrupt — A wire through which a device issues voltage, thereby signaling a request for the processor's attention.

interrupt request (IRQ) — A message sent to the computer that instructs it to stop what it is doing and pay attention to something else. IRQ is often used (informally) to refer to the interrupt request number.

interrupt request number (IRQ number) — The unique number assigned to each interrupt in a computer. Interrupt request numbers range from 0 to 15, and many PC devices reserve specific numbers for their use alone.

jumper — A small, removable piece of plastic that contains a metal receptacle that fits over a pair of pins on a circuit board to complete a circuit between those two pins.

By moving the jumper from one set of pins to another set of pins, you can modify the board's circuit, thereby giving it different instructions on how to operate.

Layer 3 switch — A switch capable of interpreting data at Layer 3 (Network layer) of the OSI Model.

Layer 4 switch — A switch capable of interpreting data at Layer 4 (Transport layer) of the OSI Model.

loopback plug — A connector used for troubleshooting that plugs into a port (for example, a serial, parallel, or RJ-45 port) and crosses over the transmit line to the receive line, allowing outgoing signals to be redirected back into the computer for testing.

managed hub — See *intelligent hub*.

memory range — A hexadecimal number that indicates the area of memory that the network adapter and CPU will use for exchanging, or buffering, data. As with IRQs, some memory ranges are reserved for specific devices—most notably, the system board.

MIB (management information base) — A collection of data used by management programs (which may be part of the network operating system or a third-party program) to analyze network performance and problems.

MicroChannel Architecture (MCA) — IBM's proprietary 32-bit bus for personal computers, introduced in 1987 and later replaced by the more standard EISA and PCI buses.

modular hub — A type of hub that provides a number of interface options within one chassis. Similar to a PC, a modular hub contains a system board and slots accommodating different adapters. These adapters may connect to other types of hubs, routers, WAN links, or to both Token Ring and Ethernet network backbones. They may also connect the modular hub to management workstations or redundant components, such as an extra power supply.

modular router — A router with multiple slots that can hold different interface cards or other devices so as to provide flexible, customizable network interoperability.

network adapter — A synonym for NIC (network interface card). The device that enables a workstation, server, printer, or other node to connect to the network. Network adapters belong to the Physical layer of the OSI Model.

open shortest path first (OSPF) — A routing protocol that makes up for some of the limitations of RIP and can coexist with RIP on a network.

passive hub — A hub that simply amplifies and retransmits signals over the network.

PC Card — See *PCMCIA*.

PCMCIA — An interface developed in the early 1990s by the Personal Computer Memory Card International Association to provide a standard interface for connecting any type of device to a portable computer. PCMCIA slots may hold modem cards, network interface cards, external hard disk cards, or CD-ROM cards. PCMCIA cards are also known as PC Cards or credit card adapters.

Peripheral Component Interconnect (PCI) — A 32-, 64-, or 128-bit bus introduced in its original form in the 1990s. The PCI bus is the network adapter

connection type used for nearly all new PCs. It's characterized by a shorter length than ISA, MCA, or EISA cards, but a much faster data transmission capability.

router — A multiport device that can connect dissimilar LANs and WANs running at different transmission speeds and using a variety of protocols. In addition, a router can determine the best path for data transmission and perform advanced management functions. Routers operate at the Network layer (Layer 3) or higher of the OSI Model. They are intelligent, protocol-dependent devices.

routing information protocol (RIP) — The oldest routing protocol that is still widely used. RIP does not work in very large network environments where data may have to travel through more than 16 routers to reach their destination (for example, on the Internet). And, compared to other routing protocols, RIP is slower and less secure.

routing protocols — The means by which routers communicate with each other about network status. Routing protocols determine the best path for data to take between nodes. They are not identical to routable protocols such as TCP/IP or IPX/SPX, although they may piggyback on top of routable protocols.

routing switch — Another term for a Layer 3 or Layer 4 switch. A routing switch is a hybrid between a router and a switch and can therefore interpret data from Layer 2 and either Layer 3 or Layer 4.

runts — Packet fragments.

single point of failure — A device or connection on a network that, were it to fail, could cause the entire network to stop functioning.

source-route bridging — A type of bridging in which the bridge polls the network to determine the best path for data between two points. Source-route bridging is not susceptible to circular routing and, for this reason, is particularly well suited to WANs.

spanning tree algorithm — A technique used in bridging that can detect circular traffic patterns and modify the way multiple bridges work together in order to avoid such patterns.

stackable hub — A type of hub designed to be linked with other hubs in a single telecommunications closet. Stackable hubs linked together logically represent one large hub to the network.

standalone hub — A type of hub that serves a workgroup of computers that are separate from the rest of the network. A standalone hub may be connected to another hub by a coaxial, fiber-optic, or twisted-pair cable. Such hubs are not typically connected in a hierarchical or daisy-chain fashion.

static routing — A technique in which a network administrator programs a router to use specific paths between nodes. Since it does not account for occasional network congestion, failed connections, or device moves, static routing is not optimal.

store and forward mode — A method of switching in which a switch reads the entire data frame into its memory and checks it for accuracy before transmitting it. While this method is more time-consuming than the cut-through method, it allows store and forward switches to transmit data more accurately.

switch — A connectivity device that logically subdivides a network into smaller, individual collision domains. A switch operates at the Data Link layer of the OSI

Model and can interpret MAC address information to determine whether to filter (discard) or forward packets it receives.

translational bridging — A type of bridging in which bridges can not only forward packets, but also translate packets between one logical topology and another. For instance, translational bridging can connect Token Ring and Ethernet networks.

transparent bridging — The method of bridging used on most Ethernet networks.

USB (universal serial bus) port — A standard external bus that can be used to connect multiple types of peripherals, including modems, mice, and network adapters, to a computer. The original USB standard was capable of transmitting only 12 Mbps of data; a new standard is capable of transmitting 480 Mbps of data.

virtual local area network (VLAN) — A network within a network that is logically defined by grouping its devices' switch ports in the same broadcast domain. A VLAN can consist of servers, workstations, printers, routers, or any other network device you can connect to a switch.

Review Questions

1. If you purchase a new desktop computer today, what kind of network adapter is it likely to require?
   a. PCI
   b. ISA
   c. EISA
   d. MCA
   e. Parallel port
2. What does "ISA" stand for?
   a. International Standard Attachment
   b. Industry Standard Architecture
   c. Industry Selected Apparatus
   d. International Standard Architecture
   e. Institutional Standard Apparatus
3. Describe the process for installing a PCMCIA network adapter.
4. In which of the following instances is a wireless network adapter most appropriate?
   a. A salesperson needs to access data on her company's server while traveling.
   b. An administrative assistant needs to share files with his supervisor in the office across the hall.
   c. A warehouse employee needs to record inventory levels in the company's database for products stored throughout the warehouse.
   d. A professor needs to distribute homework assignments to her many classes of students.

e. A marketing manager needs to run digital video product demonstrations at a trade show.

5. You have just installed a new NIC on your desktop computer, which runs Windows 2000 Professional. When you reboot the machine, you can tell that neither the sound card nor the NIC is working. You suspect that they have chosen the same IRQ. How can you confirm your suspicion?
   a. Right-click the My Computer icon, click Properties, click the Hardware tab, click Device Manager, click Network Adapter, select your adapter, and select the Resources tab.
   b. Click Start, point to Settings, click Control Panel, click Network and Dial-up Connections, then double-click the Local Area Connection icon and choose Properties.
   c. Double-click My Network Places, right-click the Entire Network icon, then click Properties.
   d. Click Start, point to Settings, click Control Panel, right-click Network and Dial-up Connections, and then click Properties.
6. Which two of the following IRQs could you probably assign to a network adapter without causing a conflict with preassigned devices?
   a. 6
   b. 8
   c. 9
   d. 11
   e. 13
7. Which IRQ is typically reserved by COM1?
   a. 1
   b. 4
   c. 6
   d. 9
   e. 11
8. You can install only one network adapter in a computer. True or False?
9. On older NICs, what type of switches enable you to change the adapter's configuration?
   a. single inline pin
   b. dual inline package
   c. dual pin set
   d. single integrated pin set
   e. single pin adapter

10. Which of the following could be a symptom of a resource conflict involving the network adapter?
    a. The computer won't power on.
    b. The computer beeps three times when it starts up.
    c. The computer presents you with an error message about a video display driver.
    d. The computer alerts you that your device is conflicting with another device on the network.
    e. The computer alerts you that the NIC device drivers have not been properly installed.
11. Which two of the following methods could allow you to change the rate at which a NIC can transmit and receive data?
    a. modifying the CMOS settings
    b. modifying the NIC's IRQ
    c. modifying the operating system's network adapter resource settings
    d. modifying the NIC's settings through the network adapter's configuration utility that manages its EEPROM
    e. modifying the network adapter's jumper settings
12. Name three enhancements or features that manufacturers might add to network adapters to improve these devices' performance.
13. To which layer of the OSI Model do repeaters belong?
    a. Physical
    b. Data Link
    c. Network
    d. Transport
    e. Session
14. What is the function of a hub's uplink port?
    a. to connect it to the server on a network
    b. to connect it to the nearest workstation
    c. to connect it to another hub
    d. to connect it to a router
    e. to connect it to a management console
15. You are a network technician working on a 10BaseT network. A coworker has been having trouble logging on to the server and asks whether you can quickly tell her if her workstation's NIC is operating properly. You do not have the NIC's utility disk on hand, but you look at the back of her workstation and learn that although the

NIC is properly installed and connected to the network, something's wrong with it. What might you have seen that causes you to come to this conclusion?

a. Its LED is blinking green.
b. Its loopback plug is improperly terminated.
c. It has two types of receptacles—BNC and RJ-45—and the wrong one is in use.
d. Its LED is not lit.
e. Its jumper is improperly set.

16. Intelligent hubs differ from passive hubs in part because they can perform which of the following functions?

a. regenerate attenuated signals
b. provide expansion ports
c. connect with other hubs in a daisy-chain fashion
d. allow more than 24 nodes on one segment
e. provide network management information

17. What kind of hub introduces a single point of failure into a network design?

a. standalone hub
b. intelligent hub
c. switching hub
d. routing hub
e. modular hub

18. What is a MIB?

a. management information base
b. multimode information basis
c. multimode integration base
d. media integration base
e. managing indicator baseline

19. At what layer of the OSI Model do bridges function?

a. Physical layer
b. Data Link layer
c. Network layer
d. Transport layer
e. Session layer

20. Before they will forward packets, bridges must be configured to accept the type of protocol (for example, TCP/IP or IPX/SPX) in use by the network. True or False?

21. How do bridges keep track of whether they should forward or filter packets?
    a. From each packet they carry, they extract source node addresses; all source node addresses that don't belong to the bridge's broadcast domain are filtered.
    b. They maintain a filtering database that identifies which packets can be filtered and which should be forwarded, based on their destination address.
    c. They hold each packet until it is requested by the destination node, at which time the bridge forwards the data.
    d. They compare the incoming data's protocol with the previous data's protocol and filter those incoming packets that don't match.
22. Which of the following is an advantage of using switches rather than hubs?
    a. Switches can provide network management information.
    b. Switches can assign dedicated channels to certain nodes, making their transmissions more secure.
    c. Switches can more accurately transmit data from one segment to another.
    d. Switches can alert the network administrator to high data collision rates.
    e. Switches do not examine Network layer protocol information, which makes them faster than hubs.
23. In cut-through switching, which frame field does the switch never read?
    a. start frame delimiter
    b. source address
    c. destination address
    d. frame check sequence
24. Which type of switching is more appropriate for heavily trafficked networks?
    a. QoS switching
    b. circuit switching
    c. store and forward switching
    d. cut-through switching
    e. message switching
25. A VLAN can be created using only one switch. True or False?
26. Which two of the following are important functions performed by a router?
    a. determine the best path for forwarding data to its destination
    b. regenerate attenuated signals
    c. separate groups of network devices into broadcast domains
    d. send broadcast signals to all network segments
    e. integrate LANs using different Network-layer protocols

27. How do routing protocols and routable protocols differ?
    a. Routable protocols contain addressing information, and routing protocols do not.
    b. Routable protocols are generated by routers, and routing protocols are interpreted by routers.
    c. Routable protocols can be interpreted by routers, and routing protocols assist routers in communicating with other routers.
    d. Routable protocols enable communication between routers, and routing protocols enable communication between all nodes on a network.
28. OSPF is a more efficient routing protocol than RIP. True or False?
29. A brouter contains characteristics of which two of the following devices?
    a. hub
    b. bridge
    c. switch
    d. repeater
    e. router
30. Why can't routers forward packets as quickly as bridges can?
    a. Routers operate at Layer 3 of the OSI Model and, therefore, take more time to interpret logical addressing information.
    b. Routers have smaller data buffers than bridges and, therefore, can store less traffic at any given time.
    c. Routers wait for acknowledgment from destination devices before sending more packets to those devices.
    d. Routers operate at Layer 4 of the OSI Model and, therefore, act as the traffic cops for all data, making them slower than bridges, which operate at Layer 3.
    e. Routers are susceptible to broadcast storms; therefore, they must periodically clear their cache and request retransmission of data that have already been transmitted.
31. Describe the difference between static and dynamic routing.
32. At which layers of the OSI Model do gateways function?
    a. Layers 1 and 2
    b. Layers 2 and 3
    c. Layers 1, 2, and 3
    d. Layers 6 and 7
    e. at all layers

33. EIGRP is a routing protocol that was developed by which company?
    a. Intel
    b. Nortel
    c. Cisco
    d. IBM
    e. 3Com
34. Which of the following routing protocols is used on the Internet's backbone?
    a. EIGRP
    b. OSPF
    c. GRP
    d. BGP
    e. RIP
35. What is the function of an e-mail gateway?
    a. It translates e-mail messages from one type of e-mail software package to another.
    b. It translates e-mail messages from one type of operating system to another.
    c. It translates e-mail messages from one type of network transport model to another.
    d. It translates e-mail messages between two or more collision domains.
    e. It translates e-mail messages between different languages.

HANDS-ON PROJECTS

Project 6-1

In this exercise, you will have the opportunity to install a PCI network adapter in a workstation, then properly configure it to connect to the network. For this project and Project 6-2, you will need a new Ethernet PCI network adapter, the floppy disk and documentation that came with it, and a desktop computer with Windows 2000 Professional installed. You will also need a Windows 2000 Professional installation CD, a Phillips-head screwdriver, and a wrist strap and mat to guard against electrostatic discharge.

1. Before installing the network adapter, turn on the PC and note the icons present on the Windows 2000 Professional desktop. Do you see a My Network Places icon?
2. Click **Start**, point to **Settings**, then click **Network and Dial-up Connections**. The Network and Dial-up Connections window opens.

3. Right-click the **Local Area Connection** icon and choose **Properties** in the shortcut menu. The Local Area Connection Properties dialog box opens.
4. Click the **General** tab, if necessary. Which components are listed as installed?
5. To make certain that you are peforming a fresh installation, you will now remove any existing network adapter drivers. Right-click **My Computer**, then choose **Properties** from the shortcut menu. The System Properties dialog box appears.
6. Click the **Hardware tab,** then click the **Device Manager** button. The Device Manager window opens.
7. In the list of installed components, double-click on **Network Adapters**. A list of your installed network adapters should appear.
8. For each installed adapter, right-click on the adapter name and choose **Uninstall** from the shortcut menu. The Confirm Device Removal window will appear, warning you that you are about to uninstall the device from your system. Click **OK** to confirm that you want to uninstall the network adapter.
9. Close the Device Manager window, then close the System Properties dialog box.
10. Click **Start**, then click **Shut Down**. The Shut Down Windows dialog box opens, prompting you to indicate your choice. Make sure the Shut Down option is selected, then click **Yes** to confirm that you want to shut down the computer. You must always shut down a workstation before installing an expansion card NIC.
11. Now physically install the network adapter in the PC as described earlier in this chapter, making sure to turn off the power before opening the case. Be sure that the network adapter is securely inserted before replacing the computer's cover. If you are unsure about whether the network adapter is pushed into the slot far enough, ask your instructor for assistance.
12. Replace the computer's cover, insert the power cable, and turn the computer on.
13. Watch the NIC's LED as the computer reboots. What does it do?
14. Does your computer start up without locking up or presenting you with error messages? Either way, proceed to Project 6-2, in which you will have the opportunity to change the network adapter's settings in the CMOS utility.

Project 6-2

In this exercise, you will view and, if necessary, change the CMOS settings for the network adapter you installed in Project 6-1. Note that each computer may require a different keystroke (for example, Del or Shift+F1) to invoke the CMOS setup utility while it starts up. Pay attention to the instructions that appear on your screen to find out the correct keystroke or combination of keystrokes.

1. Turn off the computer. Wait at least eight seconds to allow the hard disk to stop spinning, then turn on the computer again.
2. Watch the screen to find out which key or keys you need to press to enter the setup program, then press those keys.

3. You should now be in the CMOS setup utility. Because each CMOS setup utility looks different, you will have to search through the menus to find where the IRQs of PCI devices are listed.
4. Which IRQ has been assigned to your network adapter? Do you see any error messages about conflicting devices?
5. Try changing the IRQ assigned to your network adapter. Usually, you will want to highlight the current value, then press either the Page Up key, the + key, or Enter to change the value. The key you press will depend on the type of BIOS used by your computer. Read the screen to determine which key or combination of keys you should press.
6. Try changing the network adapter's IRQ to 6. Does the BIOS utility prevent you from choosing IRQ 6? If so, what message does it display?
7. Change the IRQ to a number that, according to the BIOS, does not conflict with any other devices.
8. Exit the CMOS setup utility, making sure to save your changes. (Because each CMOS utility uses different keystrokes or combinations of keystrokes, read the screen to find out how to save changed settings.)
9. Upon restarting, does the computer freeze up or display any error messages? If so, try reinstalling the network adapter from the beginning. (You may want to enlist your instructor's help with this.) Otherwise, continue to Project 6-3.

Project 6-3

Now that you have installed the network adapter (in Projects 6-1 and 6-2), you need to install the appropriate software so that you can connect to the network. In this exercise, you will allow the operating system to choose and install its drivers for the NIC, then you will update those with the drivers on the disk that came with your network adapter.

At the end of Project 6-2, you restarted your computer after installing the network adapter. Providing that you have not disabled the plug-and-play technology on your workstation, Windows 2000 should recognize the new hardware and install the device drivers automatically. The first step in this project begins at this point.

1. Once Windows 2000 reboots, the operating system will install device drivers for your new NIC.
2. Follow the steps described under the "Installing and Configuring Network Adapter Software" section of this chapter for updating NIC drivers. (*Note*: if the Update Driver Wizard informs you that the driver you are installing is older than the driver already present for the adapter, continue installing the device driver from the disk anyway.)
3. At the end of these steps your NIC should be functioning using the new device driver. Upon rebooting, verify this by viewing the NIC's LED.

Project 6-4

In this exercise, you will verify that the network adapter you installed and configured in Projects 6-1, 6-2, and 6-3 works, by viewing the device's properties through the operating system and attempting to connect to the network. (Obviously, if Windows 2000 displayed error messages pertaining to the network adapter after rebooting, it is not installed correctly. You may want to remove it, using the Add/Remove Hardware Wizard. To open this dialog box, click Start, point to Settings, click Control Panel, double-click Add/Remove Hardware, and follow the instructions. After you have removed the network adapter, change its device driver back to the one originally chosen by the operating system, or change its CMOS settings. Usually, if you can get to the point where Windows recognizes the network adapter, but still presents errors pertaining to its use of resources such as its IRQ, you can at least be certain that it is physically installed correctly.)

1. Right-click the **My Computer** icon. A shortcut menu opens.
2. Click **Properties**. The System Properties dialog box opens.
3. Select the **Hardware** tab.
4. Click the **Device Manager** button. The Device Manager window appears.
5. In the list of devices, double-click **Network adapters**.
6. Double-click the name of the adapter for which you are verifying system resources. The network adapter's Property dialog box appears.
7. Click the **Resources** tab.
8. Note the IRQ number in use by this device. Does it match the number you set through the CMOS utility in Project 6-2?
9. Close the network adapter's Property dialog box by clicking **Cancel**.
10. Close the Device Manager window.
11. Click **OK** or **Cancel** to close the System Properties dialog box.

Project 6-5

In this exercise, you will use the workstation whose network adapter you configured in the previous projects to connect to a server as part of a LAN. You will use a hub to connect the workstation and server to the LAN. If you are working in a classroom setting, your classmates will use the same hub to connect to the network, thus forming a small LAN. This project uses a Windows 2000 server and, as part of configuring your workstation to connect to this server, you will install Client for Microsoft Networks. You will configure this client so that you and your classmates belong to a Windows 2000 workgroup (that is, a group of devices).

For this project, you will need a working Windows 2000 server with valid logon IDs and a workgroup called CLASS, plus a folder called C:\TEMP established, a standalone hub, the instruction manual that came with the hub, two or more patch cables compatible with your network adapter and the hub's ports, and the Windows 2000 workstation whose network adapter you configured in the preceding Hands-on Projects.

1. Set up the hub according to the instruction manual's directions. Usually, summarized directions for installing the hub will appear at the beginning of such a manual. For a small standalone hub, setup should involve little more than connecting it to the wall outlet, making sure it lights up correctly, then connecting it to the server.
2. Connect a patch cable from one of the hub's ports (but not the uplink port) to your workstation's network adapter.
3. Connect another patch cable from the hub into the network adapter of the server.
4. On your workstation, right-click **My Network Places**, then click **Properties**. The Network and Dial-up Connections window opens. (Another way to open this window is as follows: Click **Start**, point to **Settings**, click **Network and Dial-up Connections**.)
5. Right-click the network connection that corresponds to the small network you have established with your hub, server, and workstation, then choose **Properties**.
6. The Local Area Connection Properties dialog box appears. Note the list of installed components. Click **Install** to begin installing a new component.
7. The Select Network Component Type dialog box opens. In the list of components, double-click **Client**. The Select Network Client dialog box opens.
8. In the list of network clients, click **Client for Microsoft Networks**. (If the Microsoft Client for Networks is already installed on the workstation, click **Cancel**, then **Cancel** again, and proceed to Step 11.)
9. Click **OK** to begin installing the Client for Microsoft Networks.
10. Once the Client for Microsoft Networks has been installed, you are ready to configure its properties.
11. Close the Local Area Connection Properties dialog box by clicking **OK**. Next you will identify the workstation and assign it to a workgroup.
12. Right-click the **My Computer** icon, click **Properties**, and then click the **Network Identification** tab. The computer's default name and workgroup should be visible.
13. To change these settings, click **Properties**.
14. For the Computer name, type: **Student*X***, where *X* is a unique number (if you are in a classroom; if you are not in a classroom, you can replace *X* with any number). Make sure the Workgroup radio button is selected, and underneath the Workgroup prompt type: **CLASS**.
15. Click **OK**, and then click **OK** again at the System Properties dialog box to save your changes. Click **Yes** to confirm that you want to restart the computer.
16. When Windows 2000 starts up again, type the student login ID and password that your instructor has created for you on the server.

17. After some of your classmates have completed Steps 1 through 11, double-click the **My Network Places** icon. What do you see?
18. Double-click the server's icon in the My Network Places window (You may need to navigate through the network to find your server.)
19. Open the **C:\TEMP** directory on the server and view its contents. You are now generating more traffic between the workstation and the server. Watch what happens to the lights next to the hub's port that connects your workstation.
20. Disconnect your workstation from its port in the hub while the data are being copied. What kind of error messages, if any, appear on your workstation and on the server?
21. Wait a few minutes, then reinsert the patch cable. What happens?

Case Projects

1. Evco Insurance, a multimillion-dollar life insurance firm, has asked you to help troubleshoot the network at its corporate headquarters. The network manager admits that he has not kept very close tabs on the network's growth over the last year, and he thinks this omission has something to do with the congestion problems. The Marketing Department, which is experiencing the worst network response, has added 40 people in the last six months to make a total of 146 people. At some times during the day, the marketing director has complained of waiting 10 minutes before one small e-mail message can get across the wire. He shows you to the telecommunications closet that serves the troubled department. Inside, you find a stack of eight expensive new hubs, blinking away. What are your first thoughts about why these users might be getting such poor response?
2. While you are in the telecommunications closet at Evco Insurance, you notice that one hub has two ports whose collision lights are blinking almost constantly. Being a conscientious network professional, you point out this problem to the network manager. What do you suggest you and he do next?
3. The network manager at Evco Insurance likes the fact that you have helped figure out some of his hub problems. He is especially pleased to know that he does have switching hubs and can reconfigure them to give certain users or groups of users a dedicated channel to the LAN. He thinks he might want to take this approach. The network manager understands the performance benefits that users would gain, but he still isn't sure who should get the benefit of switching. What can you tell him about switching and security that might help him decide which users' nodes should be switched?
4. The network manager at Evco Insurance understands that switches are becoming increasingly more advanced. Evco currently uses routers to connect most of its network segments to the backbone, and it uses routers to connect its 12 satellite offices around town to the corporate headquarters. The network manager asks whether you think he would be wise to replace these routers with switches in the future. What is your response?